RAY
PUBLISHING & SCIENCE

أمن الحاسب وأمان المعلومات

جواسيس الحاسب

إعداد المهندسة أناستاسيا محمد أكرم الكحالة

أمن الحاسب
وأمان المعلومات

جواسيس الحاسب

- الطبعة الأولى 2005

- الناشر: شعاع للنشر والعلوم

حارة الرباط 2 - المنطقة 12 - حي السبيل 2

تلفاكس: 2643545 (21) 00963

هاتف : 2643546 (21) 00963

سورية ـ حلب

ص.ب 7875

لمزيد من المعلومات ولشراء كتب الدار مباشرة على الإنترنت

يرجى زيارة موقعنا http://www.raypub.com

البريد الإلكتروني للقراء: quality@raypub.com

info@raypub.com

البريد الإلكتروني للزبائن: sales@raypub.com

البريد الإلكتروني لدور النشر: orders@raypub.com

أمن الحاسب
وأمان المعلومات

جواسيس الحاسب

إعداد
أناستاسيا محمد أكرم الكحالة

مقدمة

"المعلومات هي هواء العصر الحديث. فهي تسيل عبر الجدران ذات الأسلاك الشائكة، وتحلق من خلال الحدود المشحونة بالكهرباء."

اقتباس من أحد أقوال Ronald Reagan.

فكرة عن الكتاب

الأمر الذي لم يذكره المتّصل العظيم Ronald Reagan هو أنه تتم أحياناً ملاحقة البيانات بشكل كبير، ويقوم الناس تقريباً بأي شيء للحصول عليها.

ربما لا تملك شيئاً تخفيه، لكن قد يهتم الكثير من الأشخاص بمحتويات حاسبك، مثل زملاء العمل الفضوليين، المتطفلين من أفراد العائلة، المخربّين الخبيثين، الجواسيس، ضباط قوى الأمن، والأزواج الغيورين. إذا كان لديك شيء تخفيه، ماذا سوف يحصل إذا عرفوا بأمره؟

لا تحتاج إلى اتباع تدريب خاص من قبل وكالة CIA أو امتلاك ميزانية ضخمة مثل ميزانية وكالة الأمن القومي NSA لتدير عمليات التجسس الحاسبي. حيث يمكن بعملية بحث سريع على شبكة الإنترنت الحصول على مئات البرامج المتوفرة والتي يمكن لأي شخص عادي أن يشتريها، مع التعليمات الكاملة التي قد تحول الشخص العادي إلى شخصية رقمية للبطل James Bond، كما يتم استخدام هذه الأدوات يومياً للتجسس بشكل قانوني أو غير قانوني على مستخدمي الحواسب.

في الحقيقة من الصعب جداً تقدير كمية التجسس الحاسبي التي تحصل يومياً (وإذا أعطاك أحد ما رقماً تقريبياً، فلا تأخذه بعين الاعتبار لأنه سوف يكون مجرد توقع). تؤدي وسائل الإعلام عملاً جيداً جداً بنشر قضايا التجسس البارزة، لكن السبب الوحيد لانتشارها هو أنه تم اعتقال أحد ما. إلى جانب ذلك من الصعب جداً تقدير كمية التجسس التي تحدث لأنه في كثير من الحالات لا تنشر وكالات الأعمال والوكالات الحكومية محاولات التنصت الناجحة أو الفاشلة بسبب

العلاقات العامة السلبية، (حيث لا يفرح حاملو الأسهم كثيراً عندما يعلمون بأنه تم اختراق الأمن والوصول إلى معلومات عن الأبحاث والتطوير للمنتجات المستقبلية).

بالرغم من أننا لا نعلم كمية التجسس الحاسبي الذي يحصل، لكن توجد مع ذلك بعض النقاط المعروفة والتي قد تساعدنا أكثر في فهم احتمال وقوع حالات التجسس:

- يتم استخدام الحواسب بشكل متزايد لتخزين البيانات السرية والبالغة الأهمية (سواء كانت ذات طبيعة شخصية، مهنية، أو حكومية). من الأسهل والأسرع نسخ هذا النوع من البيانات مقارنة مع وسائط التخزين غير الإلكترونية مثل الورق.
- يوجد عدد كبير من نقاط الضعف على مستوى أنظمة التشغيل والتطبيقات، كما يوجد الكثير من البرمجيات سهلة الاستخدام المصممة لاستغلال نقاط الضعف هذه.
- لقد ازداد عدد الحواسب المتصلة بالإنترنت خلال السنوات الماضية، وازداد أيضاً احتمال الهجوم على هذه الحواسب من مواقع بعيدة.
- لقد أظهرت كثير من الحالات المنشورة بأن الخطر الأعظم هو من الدخلاء، ومع ذلك يتم الاهتمام بصورة أكبر بالهجمات الخارجية وهي لا تتضمن وجود شخص من الداخل يقوم بكشف بيانات حاسبك، سواء في المترل أو في مؤسسة متحدة.

عندما تبدأ بالتفكير حول جميع هذه الأمور، تدرك وجود احتمال جدي لارتباط أحد ما في الإصدار المحدّث مما نسميه ثاني أقدم مهنة في العالم. يزداد الخطر مع الكمية الكبيرة من عمليات التخريب والمعلومات وأدوات التجسس المتوفرة مباشرة على شبكة الإنترنت، مما يسهّل على أي شخص أن يصبح جاسوساً حاسبياً مبتدئاً. (فعلياً، قد تكون المخاطر من المبتدئين أكبر لأنهم أكثر، ويستطيع المبتدئ غالباً التسبب بنفس كمية الضرر التي يقوم بها الجاسوس المحترف على حاسب غير مؤمّن جيداً).

يتحدث هذا الكتاب عن الأدوات والتقنيات التي يستخدمها الجواسيس المبتدئون والمحترفون من أجل كشف البيانات، إلى جانب الإجراءات المضادة للتغلب عليها. يستخدم المخرّبون (Crackers) غالباً بعضاً من هذه التقنيات، وخاصة المتعلقة بالشبكات، لكن يعتمد عدد من الهجمات الحاسبية على امتلاك وصول فيزيائي إلى الحاسب. (تعالج كثير من كتب أمن الحواسب بإيجاز هذه الوسائل، وتقول بأنه إذا تمكن الخصم من الوصول فيزيائياً إلى الحاسب، فإن اللعبة تكون قد انتهت. أما بالنسبة لي فإنني أعتقد أن هذا الجيل واسع جداً. فمن المهم معرفة كيفية اختراق الحاسب في حال استطاع أحد ما الوصول إليه. حيث تفيدك هذه المعرفة في أن تستعد لحماية حاسبك ضد الهجمات الفيزيائية).

سوف نركز في معظم الكتاب على أنظمة Microsoft Windows (لأن نظام التشغيل Windows يتمتع بأكبر نسبة أسهم في الأسواق وهو ما يستخدمه معظم الناس). لكن هناك مفاهيم وتقنيات عامة يمكن تطبيقها على أي نظام حاسبي، لذلك إذا كنت أحد مستخدمي أنظمة Linux، OpenBSD، أو Mac، سوف تجد هذا الكتاب مفيداً.

إلى من يوَجّه هذا الكتاب

يوَجّه هذا الكتاب لأي شخص ينتابه القلق بشأن تجسس أحد ما على حاسبه. وهذا يتراوح من مستخدمي الحواسب الشخصية إلى مدراء النظام المسؤولين عن أمن مشاريع كاملة.

إذا كان عملك يتضمن جمع الأدلة من الحواسب (أي التجسس القانوني)، وكنت من ضباط قوى القانون، مدير نظام، أو فاحص شرعي، يمكن أن تضيف هذا الكتاب إلى مكتبتك.

لا تحتاج إلى تصريح سري للغاية أو خلفية قوية في التشفير أو الأمن الحاسبي لكي تستطيع أن تقرأ الكتاب. حيث سوف يجد القرّاء التقنيون وغير التقنيون معلومات مفيدة تساعدهم على تفهم مخاطر التجسس بشكل أفضل وكيفية حماية حواسبهم من جميع الأنواع المختلفة من هجمات الجواسيس.

ترتيب الكتاب

قُسمت معظم فصول هذا الكتاب إلى قسمين: "أساليب الجواسيس" و"الإجراءات المضادة". حيث يصف قسم "أساليب الجواسيس" نقاط الضعف التي يمكن استغلالها، الأدوات، وتقنيات كشف البيانات. فعلى سبيل المثال، سوف تتعلم في قسم "أساليب الجواسيس" من الفصل الرابع "اختراق النظام" كيف يستطيع الجاسوس تجاوز كلمات المرور لنظام الدخل والخرج الأساسي BIOS ومصادقة تسجيل الدخول لنظام التشغيل Windows.

سوف يُطلب منك في كثير من هذه المقاطع أن تمثل دور الجاسوس المهتم بالوصول بشكل سري إلى المعلومات. هذا لا يعني أن تكون مدرساً للمتنصتين الإلكترونيين، لكن لتدخل ببساطة في التوجه العقلي والفكري لأحد ما مهتم بالحصول على وصول غير شرعي إلى بياناتك. حيث أن التفكير بأسلوب الجاسوس المقدم على سرقة المعلومات الهامة هي طريقة فعالة جداً لاكتشاف ما عليك فعله لدعم إجراءاتك الدفاعية.

هذا ينقلنا إلى قسم "الإجراءات المضادة"، حيث سوف تتعلم ماهية الأدوات والطرق العملية للتغلب على أدوات وتقنيات الجاسوس. كمثال، سوف تتعلم حول كيفية كلمات المرور القوية، الإعدادات الأمنية لنظام التشغيل Windows، وأساليب أخرى للحفاظ على البيانات بمأمن من جاسوس يحاول اختراق نظامك وذلك في قسم "الإجراءات المضادة" من الفصل الرابع.

يتضمن الكتاب عدداً من المقاطع الجانبية (مثل المقطع التالي) تعرض قصصاً حقيقية عن الجواسيس، الأساليب التي يستخدمونها، نقاط الضعف التي يتطلعون إلى استغلالها، والإجراءات المضادة التي يمكن أن تنفذها لكي تحمي نظامك. لقد كتبت المقاطع الجانبية للإعلام، التعليم، والترفيه. كما يوجد أيضاً عدد كبير من الروابط للأدوات ومصادر معلومات مفصلة أكثر.

إجراءات مضادة: حلقة OODA

كان John Boyd قائد طائرة مقاتلة في سلاح القوى الجوية الأمريكية خلال الحرب الكورية. وقد تساءل Boyd عن سبب انتصار الأمريكيين في معظم المعارك الجوية مع الصينيين. حيث مقارنة مع طائرات F-86 التي كان يقودها الأمريكيون، كانت الطائرات المصممة في روسيا MiG-15 أسرع وأكثر مناورة. ومع أن خبرة وتدريب قائد الطائرة تشكل فرقاً مهماً، لكن كان هناك عامل آخر أثر على نسبة انتصار الأمريكيين 10:1.

من وجهة نظر الأداء، فقد استطاعت طائرات MiG-15 أن تنقلب وتدور أكثر من طائرات F-86، لكن تمتعت الطائرات الأمريكية بمجال رؤية أوضح للطيارين بالوسط المحيط بهم. إضافة إلى ذلك فإن التحكم بطائرات F-86 جعل الأمر أكثر رشاقة. بناءً على هذين العاملين وضع Boyd فرضية أن الطيار الجيد لطائرة F-86 يستطيع المراقبة بشكل أكثر فعالية ويقرر ويتصرف بصورة أسرع من طيار ذي خبرة مماثلة يقود طائرة MiG-15.

لقد ساعدت هذه الملاحظة Boyd على تطوير مفهوم يسمى OODA وهو اختصار للكلمات راقب، وجّه، قرّر، وتصرّف (Observe، Orient، Decide، and Act). وقتما يكون أحد ما في حالة يحتاج فيها إلى القرار، يقوم بالمرور دون شعور خلال حلقة OODA. حيث يراقب أولاً الموقف، ومن ثم يوجه نفسه له، يتخذ قراراً مبنياً على الخبرة السابقة، و أخيراً يتصرف.

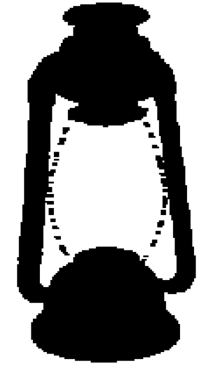
افترض Boyd أنه إذا استطعت في ظروف النزاع، أن تسرّع حلقة OODA لديك أثناء إبطاء حلقة OODA لخصمك، فسوف تنتصر. الأمر الممتع في حلقات OODA، أنه عندما تتم مقاطعة إحدى مراحل الحلقة، تعود الحلقة إلى المرحلة الأولى. فعلى سبيل المثال، إذا قاطعت حلقة خصمك بعد أن اتخذ قراره لكن قبل أن يتصرف، سوف يعود لمراقبة الوضع الجديد من الصفر.

(تابع Boyd في مساعدة تطوير الطائرة المقاتلة F-16، وتم دمج فلسفته في التكتيك والاستراتيجية في المبادئ الأساسية الحربية الحالية للمناورة في الجيش والبحرية، إضافة إلى دمجها في

نظرية الأعمال. وقد تم اعتباره كأحد ألمع الاستراتيجيين العسكريين في القرن العشرين. يمكنك الحصول على مزيد من المعلومات عن Boyd، بزيارة الموقع (www.belisarius.com).

تم تصميم هذا الكتاب لمساعدتك على تسريع حلقة OODA لديك عندما يتعلق الأمر بالتجسس الحاسبي. فعلى الأقل سوف يساعدك على توجيه نفسك بشكل أفضل حول التهديدات المحتملة، وإذا اكتشفت بأنك ضحية التجسس الحاسبي، فقد تأخذ بعين الاعتبار مختلف الإجراءات المضادة لكي تدخل إلى حلقة OODA الخاصة بخصمك محاولاً تحويل الأمور لصالحك.

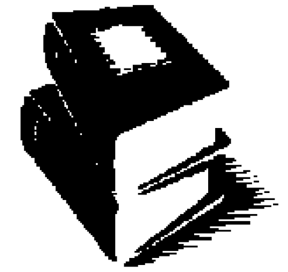
تظهر مربعات الأيقونات في النص في كل مكان خلال الكتاب، للإشارة إلى العناصر الهامة وبشكل خاص المساعدة. فيما يلي لائحة لمربعات الأيقونات ووظائفها:



تقدم هذه الأيقونة معلومات هامة أو إضافية والبيانات التقنية حول الموضوع الحالي.



تشير هذه الأيقونة إلى التقنيات المفيدة والتلميحات المساعدة لتجنب الخطر.



ترشدك هذه الأيقونة إلى المكان الذي قد تجد فيه مزيداً من المعلومات عن موضوع محدد.

بعض التحذيرات

قبل أن تبدأ بقراءة هذا الكتاب، توجد بعض التحذيرات التي يجب أن تتذكرها:

- **الروابط:** لقد كانت محددات مواقع المعلومات URL، الروابط، صفحات الويب، أو كما تفضل أن تسميها المذكورة خلال الكتاب موجودة عندما تمت طباعته. لكنك إذا كنت تستخدم الويب فإنك تعلم أن الروابط قد تكون مؤقتة لسوء الحظ. فإذا لم تعمل إحدى تلك الروابط، إلا أنه ستتوفر معلومات كافية في المقطع لاختيار جزء من النص والبحث عنه ضمن محرك البحث Google (أو أي محرك بحث آخر تقوم باستخدامه) لكي تجد ما تبحث عنه.

- **الأسعار:** توجد في كل مكان خلال هذا الكتاب مقاطع تناقش الأدوات، وأحاول أن أستعرض الأسعار لمختلف المنتجات البرمجية والتجهيزات الصلبة. حيث معظم لا تذكر الكتب أية أسعار، وهذا الأمر مضجر جداً، وخاصة عندما تجد منتجاً يناسب احتياجاتك ومن ثم تدرك أنه مكلف جداً. مع أنني أدرك أن هذه الأسعار تتقلب وسوف يكون هناك فرق في عدة أشهر بين الانتهاء من تأليف الكتاب وظهوره مطبوعاً، لكن على الأقل سوف تأخذ فكرة عامة وتقريبية حول التكاليف.

- **مصادر الأدوات:** تتوفر مصادر الأدوات التي عرضناها من خلال الكتاب على شبكة الإنترنت، لكن إذا قمت بتحميل أداة من موقع مخرّب أو حتى من بعض المواقع المحترمة، يجب أن تأخذ حذرك عبر عدد من الأمور. تأكد أنك تنفّذ برمجيات مكافحة الفيروسات وتطبيقات حصان طروادة الحديثة، وقم باختبار الأداة على حاسب لا يتضمن بيانات مهمة (ومن المفضل أنه ينفّذ تطبيق جدار الحماية Firewall) لتتأكد من أن الأداة لا تتضمن شيفرة خبيثة.

- **القانون:** في كل مكان خلال هذا الكتاب، وخاصة في الفصل الثاني، "التجسس والقانون"، سوف تجد مناقشات عامة حول مواضيع قانونية متنوعة. لكن مع ذلك إذا كانت لديك أسئلة محددة حول القوانين والعقوبات، عليك استشارة محامي قانوني مؤهل.



الجواسيس

معرفة الجواسيس

لا يرتدي جواسيس الحاسب المعاطف عادة، وكذلك لا يرتدون ملابس سوداء محكمة ولا يتعلقون بأسلاك فوق لوحة المفاتيح الخاصة بك، ومن المحتمل ألا يكون اسمهم Boris ولا يتكلمون بلهجات سلافية ثقيلة. وأغلبيتهم ليسوا حتى من القراصنة (Hackers) أو المخرّبين (Crackers)، وعلى الأرجح أنهم لا يعرفون الفرق بين العصا والألف. فإذا كان جواسيس الحاسب لا يتطابقون مع الإدراكات الشائعة لوسائل الإعلام، فمن يكونون إذاً؟

تُقسم جاسوسية الحاسب إلى هواة ومحترفين، كما هو الأمر في معظم الهوايات. فالهواة هم جواسيس عن غير قصد، مع أنهم قد يملكون أسباباً قوية للتطفل إلا أن رزقهم لا يعتمد على هذا، يملك هؤلاء خبرة بالحواسب أكثر بقليل من المستخدم العادي، لكن هذا لا يعني أنهم تقنيون جداً، إنما احتاجوا وقتاً أكثر بقليل لتعلّم التقنيات المتنوعة التي يمكن استخدامها للوصول إلى الأجهزة الحاسبية دون إذن مسبق ومن ثم تطبيق تلك المعرفة لتحقيق أغراض التجسس. إن تعلّم أدوات التجسس ثم اكتسابها هو مجرد طرف من عملية الاتصال بالإنترنت. عندما تفكر بهذه النماذج من الجواسيس، لا تتخيل شخصيات Tom Cruise أو Sandra Bullock، إنما يتمثّل أمامك رئيسك بالعمل، زميلك، زوجك، أطفالك، أو جارك.

يميل الجواسيس المحترفون إلى امتلاك خبرة تقنية أكثر من الجواسيس الهواة. إن عملية التجسس على الناس هي جانب من جوانب مهنة المحترفين. قد يكون التجسس مشروعاً، كما في حالة موظف استخبارات ينفذ أمر قضائي متعلق بجريمة قتل طفل، أو غير مشروعاً، كما في حالة جاسوس مُستأجر للحصول على معلومات حول أسرار الصفقات التجارية من شبكة تخص مؤسسة تجارية. بالرغم من استخدام هؤلاء الجواسيس لنفس الأدوات والتقنيات التي يستخدمها الهواة، إلا أنهم يمتلكون إدراك أعمق للتقنيات بالإضافة إلى الوصول لأدوات تجسس أكثر تطوراً

وتعقيداً. لا يمكنك تمييز جاسوس محترف أو جاسوس هاوٍ من خلال مظهره. لنأخذ بعين الاعتبار Aldrich Ames أو Robert Hanssen: وهما مطلعان لصالح مكتب التحقيقات الفدرالي ووكالة الاستخبارات المركزية، ذوي مظهر بريء، من الطبقة المتوسطة، وعمر متوسط، وقد قاما بعملية التجسس على الروس بنجاح لكن اندمجا مع المجتمع لسنوات طويلة. مرة أخرى لا يتطابق الجواسيس المحترفون مع النماذج الرومانتيكية الشائعة لحقيقة التجسس بين وسائل الإعلام مع أنه قد يكون أحدهم شريكاً في جريمة تسمى Natasha.

من الهام فهم مختلف أنواع الجواسيس بشكل عميق لسببين:

- فهم القيود والقدرات التقنية لخصم كامن كهذا. وهذا أمر واضح لأنك تريد التأكد أن إجراءاتك الأمنية يمكنها الصمود في وجه جاسوس محاولاً اختراقها.
- فكّر بعقل الجاسوس. نستعرض من خلال هذا الكتاب مقاطع حول وسائل التجسس، وبشكل خاص حول ما يتعلق بكيفية التجسس على الحواسب. تطلب معظم هذه المقاطع أن ترتدي معطف الجاسوس لكي تحصل على أمن أفضل، لتحمي نفسك بشكل كامل، ومع ذلك لا تحتاج إلى معرفة الأدوات والتقنيات فقط، إنما معرفة التوجه الفكري للجاسوس. هناك مَثَل شائع يقول، "ماذا كان (المسيح، غاندي، ضع مثلك الأعلى المفضل) سيفعل؟" وعندما تراجع أمنك عليك أن تسأل، "ماذا كان جاسوس مشترك (أو أي نوع آخر من الجواسيس قد يشكل تهديداً) سيفعل؟"

من أقوال الخبير الاستراتيجي العسكري الصيني الشهير Sun Tzu، "إذا عرفت عدوك وعرفت نفسك ليس عليك الخوف من مئات المعارك. إذا عرفت نفسك و لم تعرف عدوك، ستعاني بعد كل انتصار حققته هزيمة. إذا لم تعرف نفسك و لم تعرف عدوك، سوف تستسلم في كل معركة."

سيتم في هذا الفصل تطبيق مفاهيم معرفة العدو، معرفة نفسك، ومعرفتهما كليهما على عمليات التجسس على الحواسب.

ما الذي يوجد وراء الجواسيس ومن يكونون

لنبدأ بمعرفة العدو. يتعلق التجسس على الحواسب بالاستكشاف الهادف للمعلومات أو الدلائل. إذا كنت تستخدم تعريفاً معجمياً (في هذه الحالة، معجم التراث الأمريكي اللغة الإنكليزية، الإصدار الرابع)، سيكون تعريف كلمة معلومات هو "معرفة أحداث أو مواقف محددة تمّ تجميعها أو استقبالها عن طريق الاتصالات، الاستخبارات، أو الأخبار." ومن جهة أخرى تعريف الدليل هو "شيء أو أشياء تساعد على تكوين استنتاج أو حكم." قد يبحث جاسوس

صناعي عن معلومات سرية موجودة على الحاسب المحمول الخاص بمدير مشروع لشركة Microsoft وترتبط هذه المعلومات بشكل خاص بمستقبل الشركة ونظام التشغيل Longhorn. وقد تبحث زوجة تشك بأن زوجها يقيم علاقة غرامية عن دليل في رسائل البريد الإلكتروني يثبت شكوكها. قد تتطور معلومات ما إلى دليل بناء على محتواها، فعلى سبيل المثال قد يخص رقم هاتف مخزن في دفتر عناوين للمساعد الرقمي الشخصي PDA أحد تجار المخدرات المعروفين ويصبح بالتالي دليلاً مساعداً لقضية جنائية.

عليك أن تتذكر أن التجسس هو عمل هادف. بالرغم من مفاجأة الزوجة كثيرة الشك بالدليل الواضح أمامها بأن زوجها يخونها لأنه ترك بالصدفة نافذة الدردشة مفتوحة على حاسب العائلة، لا يعتبر هذا تجسساً، فعلياً لم تكن تبحث عن معلومات.

قد تكون أنواع المعلومات والدلائل التي تمّ جمعها خاصة جداً أو عامة جداً، ويعتمد ذلك على ما يحاول الجاسوس تحقيقه، ربما يبحث عن معلومات مالية ترتبط باندماج قريب وسوف يكون راضياً بالتطفل على ملفات الحسابات. ومن جهة ثانية، قد تفحص وكالة استخبارات حكومية المحتويات الكاملة للقرص الصلب الخاص بمجرم ما، باحثة عن دليل يدينه إضافة إلى معلومات تتعلق بأي جرائم مستقبلية محتملة.

هناك مفهومان هامان للتجسس على الحواسب بالإضافة إلى المعلومات والدليل: إن النشاط مرفوض ومجهول. في أغلب الأحيان لن تعطي إذناً صريحاً أو ضمنياً لأحد بأن يتطفل على حاسبك، قد تحصل استثناءات في مكان العمل حيث تقع حالات مراقبة الموظفين، أو عندما تطلع الشرطي الودود أنك لا تخفي شيئاً، لا تحتاج إلى محامي، وبالتأكيد بإمكانه الاطلاع على حاسبك. بالإضافة إلى بعض الحالات التي تقع أثناء تحقيقات تنفيذ القضاء، حيث لن تتفوه بكلمة عند حصول المحكمة على إذن لمقسم الشرطة ليقوموا بالتطفل على حاسبك بسبب قيامك بنشاطات غير قانونية ومشبوهة. تذكّر أن مرفوض لا يعني بالضرورة غير قانوني. بالرغم من أن اختراق شبكة حواسب لسرقة أسرار تجارية يُعتبر انتهاكاً واضحاً لعدة قوانين، إلا أن وضع برنامج تسجيل المحادثات على حاسب ابنك دون إذن منه لمعرفة إذا كان يتحدث مع أصدقائه عن المخدرات لا يعتبر غير قانوني، مع أنه يُعتبر غير أخلاقي للبعض.

العنصر الثاني للتجسس على الحواسب هو إذا كنت أنت الهدف، فلن تعرف ذلك إلا بعد حدوثه. فعلى خلاف مصنعي الملابس، لا يترك المتطفلون علامات على الحاسب فحواها "تطفلَ عليك الجاسوس رقم 39. يترك الجواسيس أحياناً بعض الآثار، لكنها لا تكون واضحة. أياً يكن الشخص الذي يتجسس عليك فإنه لا يرغب بأن تعرف أنه يبحث عن معلومات أو دليل. توجد استثناءات مثل برنامج مراقبة الموظفين أو نظام مراقبة البيانات الحكومي (ECHELON) (تتم مناقشته لاحقاً في هذا الفصل)، والمعروف بأنه سبب ضيق وغم للذين يقومون بتشغيله.



يُعتبر نظام ECHELON مثالاً لموقف الحكومة المتكرر حول "نظام التكتم". بالرغم من التشهير بوجود نظام ECHELON، ترفض الحكومة بثبات الاعتراف بوجوده. لمزيد من المعلومات حول نظام ECHELON ونظم مراقبة البيانات الأخرى، انتقل إلى الفصل الثالث عشر.

حتى الآن، دار الحديث حول ماذا يوجد من وراء الجواسيس، لكننا لم نقم بالإجابة على سؤال Sun Tzu حول معرفة العدو، وهذا أمر هام لأنه يزودنا بفهم عميق عن دوافعهم وطرقهم، إن التفكير السيئ هو تمرين قيّم يساعدك على حماية نفسك.

بشكل عام، يتم تصنيف الجواسيس تحت سبع فئات مختلفة:

- جواسيس الأعمال
- المدراء
- رجال الشرطة
- التحريون والمستشارون
- الجواسيس الأشباح
- المجرمون
- الوشاة
- الأصدقاء والعائلة

لنقم بجولة سريعة في عالم كل صنف من الجواسيس للحصول على رؤية أفضل من يكونون وماذا يوجد خلفهم.

جواسيس الأعمال - التجسس الاقتصادي

يمثّل التجسس الاقتصادي مشكلة كبيرة، إلا أنه غالباً ما يتم تجاهلها. لقد حذرت النشرات التجارية والمنظمات ووسائل الإعلام الإخبارية، منذ الثمانينات، من مخاطر التجسس الاقتصادي، المسمى سابقاً بالتجسس الصناعي، إلا أنه تمّ تجاهل هذه التحذيرات بشكل كامل.

لنلاحظ هذه النقاط الأساسية حول دراسة أطلقتها الهيئة الأمريكية للأمن الصناعي عام 2002، غرفة التجارة، واستقصاء الثروة لألف مؤسسة تجارية وستمائة شركة أمريكية صغيرة ومتوسطة:

- أقرّ أربعون بالمائة من الشركات التي استجابت للاستقصاء عن وقوع حوادث معروفة أو مشتبه بها عن فقدان بيانات خاصة بالشركة. (وهذا يعني قيام أحد ما من داخل أو خارج الشركة بالتجسس وسرقة معلومات الشركة).
- قُدرت خسائر المعلومات الخاصة والملكية الفكرية بما يتراوح بين ثلاثة وخمسين وتسعة وخمسين بليون دولار أمريكي.
- يبحث جواسيس الأعمال عن المعلومات، يكون هدفهم الشائع البحوث، التطوير، لوائح الزبون وما يتعلق بها من معلومات، والبيانات المالية.
- بالرغم من الآثار الكامنة لهذه المهاجمات المحتمل نجاحها، فقد صرحت نسبة خمس وخمسين بالمائة من الشركات التي استجابت لنا عن اهتمام ورائها حول خسارة المعلومات واتخاذهم التدابير الوقائية لمنع وقوع ذلك. وهذا يعني أن أعداداً كبيرة من المدراء يستخفون أو لا يدركون مخاطر وتكاليف سرقة البيانات.

لا تعاني الشركات التي تتحمل مهاجمات التجسس الاقتصادي خسائر مادية بسيطة فحسب، عليها أيضاً أن تكافح المصالح المنافسة، الرسوم القانونية في حال رفع دعوى قضائية، قلة حاملي الأسهم، وثقة الجمهور في حال الإعلان عن هجوم التجسس (الكثير لا يعلنون لهذا السبب).

لا ينحصر التجسس الاقتصادي على المؤسسات التجارية الضخمة فقط، فقد تعاني شركات أصغر في الواقع ضرراً أكبر جراء هذا النوع من التجسس، كما يخضع لهذا التجسس من أشهر الباعة بالتجزئة إلى المصنّعين المبتدئين الذين يعملون ضمن نطاقات أضيق دون وجود مخزون مالي كما في الشركات الأضخم.

المنفذون المعتادون لعمليات التجسس الاقتصادي هم الموظفون السابقون، المنافسون المحليون والأجانب، والمقاولون في موقع الشركة. (من الجدير بالذكر أن هناك فارق كبير بين التجسس الاقتصادي والاستخبارات المنافسة، حيث تُمارس الاستخبارات المنافسة أو العمل باستخدام طرق مشروعة وواضحة، بينما يهدف التجسس الاقتصادي إلى استخدام الطرق غير القانونية للحصول على المعلومات. من الممكن أن تكون هناك أشياء غامضة، لكن معظم محترفي الاستخبارات المنافسة مخلصون لمجموعة ثابتة من الأخلاق دون أي تحيز).



لمزيد من المعلومات حول الفوارق بين التنافس الشرعي الذكي والتجسس غير الشرعي قم بزيارة موقع جمعية المحترفين الأذكياء التنافسية على شبكة الانترنت www.scip.org.

بالرغم من أن الأفلام والبرامج التلفزيونية تصوّر الجواسيس المشتركين، الذين يخترقون بمهارة مواقع محمية بشكل كبير، بصورة جشعة ومبهمة، إلا أن الحقيقة تكمن في أن الأشخاص الذين يكونون في مراكز تتيح لهم الإطلاع على معلومات غير محمية هم من يتحمل مسؤولية عمليات التجسس في الشركة، كما يمثل الموظفون الحاليون أو السابقون بدافع الطمع أو الانتقام تهديداً أكبر بكثير من جواسيس محترفين يعملون لصالح منافس ما.

جواسيس: مؤسسة Niku التجارية تقاضي شركة Business Engine

هاجمت مجموعة كبيرة من عملاء مكتب التحقيقات الفدرالي مكاتب شركة Business Engine في أغسطس (آب) عام 2002. Business Engine شركة برمجيات متخصصة في تطوير أدوات مشاركة على الويب، لقد تم الهجوم عند اكتشاف شركة Niku المنافسة وجود تسجيلات على ملقمها تشير أن أحداً ما ذا عنوان IP عائد لشركة Business Engine استخدم الكلمات السرية الخاصة بشركة Niku للوصول إلى شبكة الشركة أكثر من ستة آلاف مرة. لقد تم تحميل أكثر من ألف مستند خلال الاقتحام، ومنها معلومات حول الميزات القادمة، لوائح عن الزبائن السريين، الأسعار، وجداول المبيعات.

أعلنت التحقيقات اللاحقة أنه منذ شهر أكتوبر (تشرين الأول) عام 2001، اقتحم الدخلاء شبكة Niku الداخلية مستخدمين كحد أقصى خمسة عشر حساباً وكلمة سر للوصول إلى المستندات المطلوبة.

وفي أواخر شهر سبتمبر (أيلول) عام 2002، كانت شركة Niku على حافة انهيارها، بعد أن كانت أعمالها مزدهرة، بسبب انخفاض قيمة الأسهم في بورصة NASDAQ، ولم يذهب الحائز على ماجستير في إدارة الأعمال من جامعة Harvard إلى التفكير أن الحملة القضائية المكثفة ضد التجسس الاقتصادي كانت قد ساهمت في الآثار السيئة على ثروة الشركة.

رفعت شركة Niku دعوى قضائية ضد شركة Business Engine، وسيكون من الممتع مراقبة تفاصيل هذه القضية المنبثقة.

لا تنحصر مشكلتنا على الموظفين الصغار فقط. حيث استقال Jose Ignacio Lopez، وهو رئيس المشتريات في شركة General Motors، بشكل غير متوقع عام 1993 وتعاقد مع شركة Volkswagen، اتهمت شركة GM لاحقاً Lopez بتدبير سرقة أكثر من عشرين صندوق يحوي مستندات بحث، مبيعات، وتسويق. لقد تم تضمين مخططات تفصيلية لوحدات تجميع، على أمل أن شركة GM ستسيطر وتستبدل وجود شركة VW في أسواق السيارات الصغيرة. أغلقت

القضية عام 1997 عند اعتراف شركة VW وحسمت القضية المدنية بدفعها مئة مليون دولار أمريكي لشركة GM وعرضها بأن تشتري أجزاء من الشركة بقيمة بليون دولار أمريكي خلال السنوات السبع المقبلة. أسقط أخيراً الدعاة الألمان تهم التجسس الاقتصادي الموجهة إلى Lopez، لكن مع إصدار أمر بأن يتبرع بقيمة ربع مليون دولار أمريكي للجمعيات الخيرية.

ومع ذلك هناك حالات لمهاجمات خارجية وتقع من قبل موظف أو عميل لطرف منافس. تُصنّف المهاجمات الخارجية في فئتين:

- **المهاجمات الانتهازية.** قد يلاحظ العدو بشكل غير متعمد إذا كان الوصول إلى المعلومات سهلاً، بمعنى آخر محاولة لفتح الباب لمعرفة إذا كان مقفلاً. تتم سرقة المعلومات في حال كان احتمال اكتشاف السرقة ضئيلاً أو لا يتطلب جهداً. لنأخذ مثالاً على هذا النوع من المهاجمات جاسوس يستخدم منفذ الماسح الضوئي أو أي أداة تحديد غير محمية لمعرفة وجود الثغرات التي يمكن تجاوزها للدخول إلى شبكة الشركة، وفي حال العثور على ثغرة يمكنه أن يقوم بعمله.
- **المهاجمات المستهدفة.** الهجوم المستهدف هو محاولة جدية لسرقة المعلومات، يملك الجاسوس هدفاً محدداً ويستخدم تقنيات مختلفة للوصول إلى مراده. عندما تكون الحصص النقدية كبيرة، تودع كمية كبيرة من المال والموارد على عملية التجسس.

بسبب استخدام الحواسب لتخزين جميع أنواع المعلومات الخاصة بالشركة، فهي تمثل هدفاً أساسياً لجواسيس الأعمال، الشبكات، الحواسب المحمولة، الحواسب المكتبية، وأجهزة المساعد الرقمي الشخصي جميعها معرضة لهكذا مهاجمات. تتراوح المهارات التقنية التي يستخدمها جواسيس الأعمال من هؤلاء الذين يتمكنون من الوصول إلى الأجهزة الحاسبية دون إذن مسبق ومن دون امتلاك مهارات متقدمة مثل القيام بنسخ ملف موثوق إلى قرص، إلى تقنيين خبيرين والذين يستطيعون بسهولة اجتياز الجدار الناري للوصول إلى شبكة الشركة.



توجد عقوبات صارمة للتجسس الاقتصادي في الولايات المتحدة الأمريكية. انظر الفصل الثاني لمزيد من التفاصيل.

المدراء - مراقبة الموظفين

تنتشر ظاهرة مراقبة الموظفين في الولايات المتحدة الأمريكية بسرعة، فقد صرحت نسبة سبع وسبعين بالمائة من الشركات الرئيسة في أمريكا، خلال استقصاء حول مراقبة مكان العمل لجمعية

الإدارة الأمريكية AMA عام 2001، أنها قامت بمراقبة وتسجيل اتصالات ونشاطات موظفيها الحاليين، وقد تضاعفت هذه النسبة مقارنة مع أول استقصاء مراقبة أجرته وتم إصداره عام 1997.

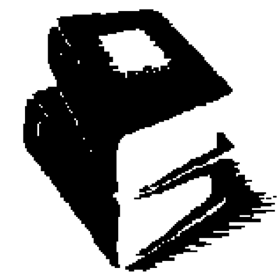
إذا كنت تعمل لصالح شخص آخر فهناك احتمال كبير أن يكون مديرك يتجسس عليك، وهذا يعني أن البريد الإلكتروني، تصفح الويب، التراسل الفوري، والأقراص الصلبة كلها قد تخضع للتدقيق. الحقيقة هي أن خصوصية الموظف لا تساهم في نتيجة العمل بل تنحدر إلى ما دون ذلك. يهتم أصحاب العمل بإيجاد دليل يثبت عدم كونك منتجاً بما فيه الكفاية أو تنتهك بطريقة أو بأخرى سياسة الشركة.

كيف تنجو الشركات بفعلتها هذه؟

عندما تتعامل مع مؤسسة حكومية، يكون لديك مجموعة من الحقوق الدستورية التي تحمي خصوصيتك، لكن لا يتم تطبيق هذه الحقوق في أمكنة العمل الخاصة، لأنك وببساطة شديدة تتقاضى راتبك من المدير والأجهزة الحاسبية التي تستخدمها تعود للشركة، فلا تتوقع أبداً أي خصوصية عندما يتعلق الأمر بنشاطاتك على الحاسب.

بإمكان صاحب العمل أن يتنصت على حاسبك، هاتفك، استراحاتك، أو أي شيء آخر تستخدمه في الشركة، بمجرد أن لديه فضولاً قوياً عما تفعله أثناء عملك لأسباب قانونية، إنتاجية، أمنية، ومعرفة أدائك في العمل.

تتم عملية المراقبة إما من الحاسب الملقم، حيث بإمكان المدراء تصفح تسجيلات الدخول والخروج أو تفحص الرسائل الإلكترونية المتبادلة، أو من خلال الحاسب المكتبي حيث يمكن تثبيت برنامج مراقبة لوحة المفاتيح.



سوف نناقش مفهوم مسجلات المفاتيح بالتفصيل في الفصل الثامن.

يتمتع موظفو المعلوماتية المشتركون في الشركة أو مستشار من خارجها بمهارات تقنية، وهم المسؤولون عن تنفيذ برنامج المراقبة. تصور مثلاً أنك حاولت أن توقف برنامج مراقبة الموظفين، سينتهي الأمر أنك ستسترعي الانتباه إلى نفسك وتقبل تحدياً شخصياً لمدير نظام مضجر لترى ما بإمكانك أن تفعل.

جواسيس: التطفل المبرر

تنتشر ظاهرة مراقبة الموظفين كثيراً في أمريكا، سواء من خلال استخدام أجهزة تصوير الفيديو، تسجيل المكالمات الهاتفية، أو مراقبة أجهزة الحواسب.

من أحد العوامل المحفزة لهذا الأمر، أنه قد حكمت عدة محاكم محلية، حكومية، وفدرالية أن أصحاب العمل مسؤولون عن الأخطاء التي يقترفها الموظفون العاملون لديهم أثناء عملهم. تستخدم الشركات برامج المراقبة والتنصت لهذا السبب، كما يبرر المدراء مراقبة مكان العمل كجزء للمساهمة في تقليص المسؤولية القانونية.

كان هناك عدد من قضايا التنصت التي أثارت ضجة كبيرة. في عام 1995 تمت مقاضاة موظف مساعد في شركة Chevron للمضايقة الجنسية المستمرة عبر البريد الإلكتروني والتي جالت في أنحاء الشركة تحت عنوان "خمسة وعشرون سبباً تجعل الجعة أفضل من امرأة." حُسمت المسألة لقاء مليونين ومائتي ألف دولار أمريكي، وتقوم الشركة حالياً بمراقبة البريد الإلكتروني لموظفيها. وفي شهر تموز عام 2000 طردت شركة Dow للكيماويات خمسين موظفاً وعاقبت مائتين آخرين لقيامهم باستعراض صور خلاعية عبر الإنترنت. وفي شهر تشرين الأول عام 1999 تم طرد أربعين موظفاً يعملون لصالح شركة Xerox لاستعراضهم مواقع ويب ممنوعة (تراقب الشركة الآن استخدام شبكة الويب من قبل أكثر من تسعين ألف موظف يعملون لديها في مختلف أنحاء العالم).

لقد أصبحت ظاهرة مراقبة الموظفين أداة إدارية منتشرة، سواء أحب الموظفون ذلك أم لا.

بالرغم من الآثار الثانوية الناتجة عن مراقبة الموظفين، تظل الشركات المسؤولة صريحة حول ذلك. يجب أن تُروّج برامج المراقبة في كتيبات الموظفين، اتفاقيات التوظيف، وعناوين الحواسب، من البديهي أن إطلاع الموظفين عن وجود برنامج مراقبة في مكان العمل هو الرادع الأفضل ضد السلوك السيئ من جعل الأمر سرياً.

من المحتمل أن تحمل السنوات القادمة تشريعاً حكومياً للزيادة من خصوصية مكان العمل، لكن من الهام حالياً إدراك أنه أثناء وجودك في العمل قد يتم اقتحام خصوصيتك الإلكترونية تحت حرية تصرف المدير، مع وجود إجراءات مضادة بإمكانك أن تتخذها ضد المدراء المتطفلين، فالحل الأفضل هو الفصل ببساطة الحياة الشخصية عن النشاطات الإلكترونية اليومية في عملك.

رجال الشرطة - تحقيقات القضاء

بعيداً عن عمليات مراقبة الموظفين، يُطبق نوع آخر من التجسس المشروع من قبل منفذي القانون. إن عدم اعتبار معظم رجال الشرطة أنفسهم جواسيس أو تفكيرهم أنهم لن يتورطوا بالجاسوسية، أمر يتعلق بعلم الألفاظ والدلالات. المصطلحات نشاطات الاستخبارات، المراقبة، والتحقيقات مقبولة أكثر من قبل المجتمع كبديل عن التجسس.

ينصب الاهتمام الأساسي لرجال الشرطة إيجاد دليل يثبت قيامك بارتكاب جريمة ما، من وجهة نظر الحاسب، قد يُجمع الدليل قبل أو بعد اتهامك بالجريمة.

إذا كنت تحت إجراءات التحقيق، قد تتم مراقبة نشاطاتك الشبكية (بما فيها البريد الإلكتروني، المراسلة الفورية، وتصفح الويب)، وقد يملك الضباط تحت ظروف خاصة حق الوصول الفيزيائي إلى حاسبك الشخصي لاستعراض محتوياته أو تثبيت برنامج تنصت أو تجهيزات مراقبة.

إذا كنت متهماً بجريمة ما فمن المؤكد أنه سيتم الاستيلاء على حاسبك وسيعاني فحصاً شرعياً لمحتوياته، يقوم تقني متخصص خلال هذا الفحص بالبحث في الأقراص الصلبة وفي وسائط التخزين الأخرى عن دليل يدينك أو يرتبط بجرائم محتملة أخرى.



الفحص الشرعي للحاسب، وهو عملية جمع الدلائل من الأجهزة الحاسبية، ستتم مناقشته مطولاً في الفصل الخامس.

يتقيد رجال الشرطة بمجموعة صارمة جداً من القواعد والإرشادات، في الأمور التي تتعلق بالتجسس على الحواسب، أصدر الدستور عدداً من الحقوق لصالح المواطن لحمايته من التدخل الحكومي غير المعقول، سواء كان مجرماً أم لم يكن كذلك. تحتاج هذه الحماية، لتحقيقات القضاء، الحصول على أمر من المحكمة أو رخصة بحث يصدرها القاضي قبل إمكانية بدء أعمال فحص الحاسب.

حصل الكونغرس الأمريكي، في أعقاب مجموعة من الهجمات الإجرامية عام 2001 على سلطات واسعة لإجراء التحقيقات من قبل وكالات تنفيذ القضاء.



سوف تناقش في الفصل الثاني السلطات الموسعة بموجب المرسوم الوطني الأمريكي (USAPA) بسبب ارتباطها بالتجسس على الحواسب.

لقد خرج ضباط القانون الفرديون فيما مضى عن السلطات الممنوحة لهم وخرقوا القانون، بالرغم من ضرورة إتباع قواعد قانونية صارمة لجمع الأدلة، وهذا يحصل إما بالصدفة أو عن سابق تصميم. أحد الأمثلة تسرب مذكرة سرية داخلية تخص مكتب التحقيقات الفدرالي في شهر تشرين الأول عام 2002، تصف محتوياها "الأخطاء المرتكبة،" مثل إيقاف البريد الإلكتروني لمواطن بريء، تسجيل مكالمات هاتفية خاطئة، تصوير المشتبهين بصورة غير قانونية، والقيام بعمليات بحث مرفوضة. مع أنه تلتزم الوكالات القانونية معظم الأحيان بمجموعة من القوانين، لا تتفاجأ إذا لم تفعل هذا في بعض الأوقات.

تختلف إمكانية كون الشرطي متمكناً من التجسس على أجهزة الحاسب بشكل هائل. بصورة عامة تفتقر الوكالات القانونية إلى التقنيين ذوي الخبرة والمعرفة لتجميع وتحليل الدليل الإلكتروني بشكل فعال. عندما يتعلق الأمر بالحواسب لا يظهر رجال الشرطة بهذا الذكاء، أما الأقلية من الأذكياء منهم مثقلون بعدد من القضايا الضخمة مع المحامين حيث يتم استخدام الدليل الإلكتروني. تسعى وكالات الشرطة إلى توظيف ضباط ومن ثم إرسالهم إلى الخارج ليحصلوا على تدريب كاف يمكنهم من أداء مهامهم الجديدة. ينجذب قليل من الأشخاص ذوي المهارات في مجال الحاسب وجمع الأدلة إلى الوكالات القانونية، بسبب وجود مناصب ذات راتب أعلى في القطاع الخاص والفروق بين الشرطة والثقافة التكنولوجية عالية المستوى.

كقاعدة عامة كلما كانت وكالة الشرطة أوسع، كلما زاد احتمال وجود خبير يتعامل مع الحواسب. تملك الوكالات القانونية الفدرالية مثل مكتب التحقيقات الفدرالي والخدمة السرية أفضل الأطقم المدربة، لكن مرة أخرى المهارات تختلف على الصعيد الفردي.

مضبوط: هل هو شرطي جيد، أم سيئ؟

استمر مكتب التحقيقات الفدرالي تحقيقاته حول مجموعة من عمليات السطو على مواقع التجارة الإلكترونية خلال صيف عام 2000، حيث تمت سرقة معلومات بطاقات الاعتماد، وقد أشار الأثر إلى مخربين (Crackers) من روسيا.

لقد كان العميل الخاص لمكتب التحقيقات الفدرالي Michael Schuler على علم تام بالمشتبهين وقد خطط لعملية احتيال متقنة للقبض على المجرمين. في شهر تشرين الثاني (نوفمبر) عام 2000، قدم كل من Vasily Gorshkov و Alexey Ivanov إلى الولايات المتحدة الأمريكية لإجراء مقابلات لطلب توظيف في شركة Invita الواقعة في Seattle وهي شركة متخصصة بأمن الحواسب. طلب موظفو الشركة من الاثنين أن يستعرضا مهاراتهما، قام كل منهما بتسجيل الدخول إلى أجهزتهما الحاسبية في مدينة Chelyabinsk في روسيا، وبدلاً من

الدخول إلى خيارات التخزين وجدوا أنفسهم أمام جدار ناري. شركة Invita هي شركة مزيفة من قبل مكتب التحقيقات الفدرالي، أما الموظفين فقد كانوا كلهم من عملاء المكتب.

لم يدرك Gorshkov و Ivanov ذلك، حيث قام العملاء الفدراليون بتثبيت برنامج sniffer على الحاسب الذي قاما باستخدامه للوصول إلى أجهزتهما في روسيا، ومباشرة بعد اعتقال الاثنين قام Schuler باستخدام الحسابات التي التقطها برنامج sniffer للدخول إلى أجهزة المجرمين وتحميل معلومات وصل حجمها إلى 250 غيغابايت كدليل قاطع يربطهما بعمليات السطو وعمليات الاحتيال من خلال بطاقات الاعتماد.

حصل Schuler على وسام لكونه أول عميل فدرالي قام باستخدام التقنية الإلكترونية لحجز ممتلكات من خارج البلاد، ومن ناحية ثانية لم تصدر أية رخصة للبحث قبل البدء بتحميل المعلومات (تم إصدارها بعد ذلك)، ولم يتخاطب أحد من مكتب التحقيقات الفدرالي مع سلطة القانون في روسيا. ناقش محامي Gorshkov هذه النقاط وكون أنه تم انتهاك القانون الروسي، لكن أصدر القاضي حكماً أن القانون الروسي لا يطبق على نشاطات العملاء.

بعد مرور عامين تقريباً، في آب (أغسطس) عام 2002، اتهمت الخدمة الأمنية الفدرالية الروسية Schuler FSB بالدخول المرفوض للحواسب في روسيا وبدأت بإجراءات قضائية ضده، من المحتمل أن تُحل القضية بصورة دبلوماسية، ومن المؤكد أن Schuler لن يرغب بقضاء إجازته في أوروبا الشرقية في المستقبل القريب.

تم إصدار حكم Gorshkov، في شهر تشرين الأول (أكتوبر) عام 2002، بقضاء مدة ثلاث سنوات في السجن مع دفع تعويض مالي بقيمة ستمائة وتسعين ألف دولار أمريكي، وقد اعترف Ivanov بعدد من التهم في شهر آب (أغسطس) عام 2002، وقد صدر حكمه في منتصف شهر آذار من عام 2003.

التحريون والمستشارون - التحقيقات السرية

يمثل المحققون السريون والمستشارون التقنيون نوعاً آخر من الجواسيس الذين قد يقومون بعمليات شرعية أو غير شرعية من التجسس الإلكتروني. يبحث هؤلاء المختصون عن الدليل الذي يرتبط بمسائل جنائية أو مدنية، وقد يتم استخدامه للأعمال، عمليات تنفيذ القانون، أو الأفراد. يتمتع التحريون بخلفيات تحقيقية رسمية، مكتسبة عادة من خلال التعامل مع أنواع مختلفة من القضايا. كما يسعى المستشارون إلى اكتساب معرفة تتعلق بمجالات تقنية متخصصة وبشكل خاص مجالات شبكات الحواسب وإجراء الفحوصات الشرعية.

التحريون

بالرغم من أن شخصيات رجال الشرطة السرية في المعاطف السوداء قد حُفرت في الثقافة الأمريكية، إلا أنه قد تغير مفهوم التحري منذ ذلك الوقت، ويرتبط بشدة الآن بالتحقيقات المرتبطة بالحواسب.

لقد ارتبط التحريون لوقت طويل بنشاطات مراقبة الصوت والصورة، ومن الطبيعي بالنسبة إليهم أن يتابعوا التقدم لنشاطات مراقبة الحواسب، إلا أن المحققون التقليديون الذين يأتون غالباً من الوكالات القانونية يتمتعون بمهارات حاسبية ضئيلة. بصورة عامة، سيقوم المحقق الخاص العادي والذي يتمتع ببعض المهارات التقنية الحاسبية باستخدام أدوات تجسس شائعة وسهلة الاستخدام. ومن ناحية ثانية سيتمتع الجيل الجديد من التحريين السريين والذي قضى وقتاً أكثر في استخدام الحواسب بمهارات تقنية تفوق مهارات الآباء والأجداد.

جواسيس: بوابة النفايات

استخدمت شركة قواعد المعطيات العملاقة Oracle، في عام 2000، تحريين من المجموعة العالمية للتحقيق IGI بهدف التحقيق والبحث في منظمتين: المعهد التعليمي المستقل وجمعية التقنية المنافسة ACT. (يعمل لصالح المجموعة IGI عدد من العملاء الفدراليين السابقين الذين اكتسبوا سمعة سيئة لقيام الرئيس Bill Clinton باستخدامهم للتحقيق في أمور تتعلق بـ Paula Jones و Monica Lewinsky). جرت هذه الأحداث أثناء إجراء تحقيقات مكافحة الاحتكار لشركة Microsoft، وقد عُدّت المنظمتان اللتان تدعمان شركة Microsoft بقوة دون أرباح مقابلة، بأنهما تملكان روابط مالية مع شركة Redmond، واشنطن.

خلال فصل الصيف، عرضت امرأة، تقول أنها تحر خاص تحت اسم Blanca Lopez، سبعمائة دولار نقداً لحراس بناء شركة ACT لتتمكن من الدخول عبر قسم النفايات في البناء، وقد استطاعت Lopez الدخول إلى البناء المقفل باستخدام بطاقة تخص Robert Waters، تحري خاص يعمل لصالح مجموعة IGI، والذي قام باستئجار مكتب تحت اسم التقنيات الصاعدة في نفس الجناح التنفيذي لشركة ACT.

صرحت شرطة واشنطن، بعد إذاعة القصة، عن عدم وجود أحد تحت اسم Blanca Lopez يعمل كتحري خاص في المدينة، وقد طرح الصحفيون المحققون في القضية أسئلة تتعلق فيما إذا كان مكتب التقنيات الصاعدة هو مجرد واجهة، هدفها الوحيد هو تغطية كونها في نفس البناء مع شركة ACT.

اعترف كل من Larry Elison وشركة Oracle باستخدامهم مجموعة IGI، مبررين هذا بأنه كان الوسيلة الوحيدة لفضح شركة Microsoft، ولكنه تجنب بحذر قضية النفايات بقوله "أنا مستعد أن أرسل نفاياتنا إلى Redmond، وبمقدورهم أن يتفحصوها."

ما حصل في الواقع، أن شركة Oracle صدقت كلاً من ACT والمعهد التعليمي المستقل، اللذان يدّعيان كونهما مجموعات تأييد مستقلة، بينما تبين كونهما منظمنين تدعمان شركة Microsoft مكلفتين بالتأثير على الرأي العام لصالح الشركة أثناء محاكمتها ضد مكافحة الاحتكار. وقد حصل أحد الأشخاص على معلومات من مجلة Wall Street بعد حادثة المال للنفايات، وتمكن الصحفيون من ربط العلاقة بين شركة Oracle ومجموعة IGI، صرحت Oracle أن مجموعة IGI أبلغت الشركة أنها سوف تستخدم تقنيات تحقيق شرعية مائة في المائة. استرعت هذه الحادثة انتباه وسائل الإعلام القومية لمدة أسبوع أو اثنين فقط.

إجراءات مضادة: خمسة فحوصات شرعية ضخمة

قد يكون اعتقادك بأن المستشارين التقنيين هم عبارة عن أشخاص مملين ويعملون بشكل فردي وحر مع ميل نحو علوم أمن الحاسب، اعتقاداً خاطئاً. لقد أصبحت الفحوصات الشرعية المتعلقة بالحاسب سلعة رائجة، في أيامنا هذه، وخاصة بالنسبة للمؤسسات التجارية الضخمة والتي تستغل هذه السلعة عند الطلب.

لنأخذ على سبيل المثال شركة الحسابات الكبيرة Deloitte & Touche والتي تؤيد التسهيلات في منطقة Boston والملقبة بالاسم "War Room"، ويحتوي المختبر على أجهزة ومعدات حاسبية معقدة بقيمة تفوق نصف المليون دولار أمريكي، والتي تستخدم لتحقيقات الزبائن على الحواسب. يستطيع التقنيون معالجة الأقراص الصلبة المتضررة والتغلغل إلى داخلها بحثاً عن الدليل القاطع، حيث عمل هؤلاء الأشخاص مع أنواع مختلفة من الجرائم ابتداءً من التحقيقات في جرائم الأغنياء انتهاء بجرائم القتل.

العمل منهك جداً، حيث يتم التعامل مع حوالي مائتين وخمسين قضية في السنة.

كقاعدة عامة، لا يمتلك التحريون الخاصون مهارات تقنية كبيرة كتلك التي قد يمتلكها جواسيس آخرون باستثناء الهندسة الاجتماعية، نعرّف مفهوم الهندسة الاجتماعية (Social Engineering) وفقاً للتحقيقات الخاصة بأنها "حجة"، ووفقاً لعمل القانون فهي استخلاص المعلومات بشكل ودي من أحدهم، حيث قد تكون الاستفادة من الطبيعة الإنسانية مدمرة بنفس مستوى الدمار الذي يحدثه اقتحام تقني محترف.

المستشارون

يدرك العاملون في الوكالات القانونية مع مرور الوقت بأنهم لا يمتلكون الخبرة الضرورية أو المهارات الفعالة فيما يتعلق بالاقتحام الشبكي وجمع الأدلة الإلكترونية، وقد نما النشاط الاستشاري الحاسبي بشكل هائل في السنوات المنصرمة الأخيرة، استجابة للعدد المتزايد من المهاجمات على الحواسب بالإضافة إلى ترويج وسائل الإعلان.

يتم استخدام مستشارين ذوي خبرة عالية للقبض على الجواسيس، وسد الطرق المختلفة لمنعهم من سرقة المعلومات، كما يُستخدمون أيضاً لإجراء الفحوصات الشرعية على الحواسب. نموذجياً، يمتلك المستشارون شهادات في علوم الحاسب وشهادات صناعية متنوعة.

من الممكن بالطبع استخدام المهارات الموظفة للقبض على جاسوس في عملية التجسس أيضاً، بالرغم من أن معظم المستشارين والتحريين هم أشخاص أخلاقيون ويتقيدون بالقانون الذي يحميك من التجسس الإلكتروني، إلا أنه توجد دائماً استثناءات لأشخاص خارجين عن القانون ويعملون مقابل أجر. ومن الجدير بالذكر أن المستشار غير الأخلاقي هو من أصعب أنواع الجواسيس التي يمكن التقاطها بسبب مهاراته ومعرفته العميقة.

الجواسيس الأشباح - تجمع استخباراتي برعاية الحكومة

عندما نسمع الكلمة "جاسوس"، يتصور المرء عملاء حقيقيين يعملون لصالح الحكومة، يحملون بطاقات الهوية، ويستمتعون بمغامرات سرية مثيرة. في عالم الجواسيس، يلقب هؤلاء بالجواسيس الأشباح، ويزاول الجواسيس الأشباح ما كان يسمى بثاني أقدم مهنة في العالم تحت وصاية الحكومة، وهم ماهرون جداً في هذه المهنة.

تكون مهمة الجاسوس في أغلب الأحيان مضجرة ومملة، عليك نسيان James Bond أو حتى Austin Powers في هذا الأمر. يكمن التجسس في تجميع معلومات سرية ومفتوحة المصدر، في محاولة لاكتشاف أحجية محيرة عما يحدث ومن ثم محاولة التغيير إيجابياً لصالح الحكومة.

تبارت وكالات الاستخبارات لبلدان مختلفة مع بعضها محاولة استكشاف أسرارها السياسية والعسكرية، وبالرغم من أن الوضع مازال على حاله، إلا أن وكالات الاستخبارات في جميع أنحاء العالم تسعى لإيجاد طرق جديدة لتبرير وجودها مع نهاية الحرب الباردة. الاستخبارات الاقتصادية ومكافحة الإرهاب هما مهمتان حديثتان وخاصة الأخيرة والتي تلقت تأكيداً كبيراً.

تكون عمليات التجمع الاستخباراتي إما مستهدفة أو عامة (مثلاً، البحث عن معلومات محددة حول نوع معين من القذائف، وتجميع معلومات عامة حول النظام الكامل للدفاع بالقذائف).

إذا كانت وكالة استخبارات مهتمة بمعلومات تعرفها، سوف تمضي الوقت بحثاً عن نقاط ضعفك وعن أفضل أسلوب لاستخلاص المعلومات منك بشكل سري.

تسلك برامج أخرى مثل برنامج ECHELON منحى مختلفاً، حيث يتم تجميع البريد الإلكتروني والاتصالات الإلكترونية عبر الإنترنت في كتلة، ثم يتم تخزينها وتحليلها بحثاً عن كلمات مفتاحية ذات أهمية، وبما أن ECHELON هو برنامج تعاوني لمشاركة البيانات، قلت الحاجة إلى أسباب وضمانات محتملة، مثلاً تجمع استراليا معلومات عن مواطن أمريكي ومن ثم ترسلها إلى وكالة استخبارات أمريكية.



لمعلومات كاملة حول ECHELON وبرامج مراقبة حكومية أخرى، انظر الفصل الثالث عشر.

إذا اهتمت وكالة استخبارات بك أو بشركتك، فاعلم عن استخدام موارد كثيرة ضدك (تقنيون محترفون، تجهيزات، وجواسيس).

في البيت

يتكون المجتمع الاستخباراتي من ثلاث عشرة منظمة ووكالة حكومية والتي تنفذ النشاطات الاستخباراتية في حكومة الولايات المتحدة الأمريكية. تتضمن الوكالات التي تقوم بالتجسس أو ترد على التجسس وزارة الخارجية، وزارة الطاقة، وزارة المالية، مكتب التحقيقات الفدرالي، مكتب الاستطلاع الوطني، وكالة التخطيط الوطنية، استخبارات القوات البحرية، الاستخبارات البحرية، استخبارات القوات المسلحة، وكالة الأمن القومي، وكالة الاستخبارات الدفاعية، ووكالة الاستخبارات المركزية.

قامت وكالة الاستخبارات المركزية وأعضاء آخرين من المجتمع الاستخباراتي بالتجسس على المواطنين الأمريكيين، حتى منتصف السبعينات، بصورة غير شرعية. بالرغم من الحظر القانوني لمراقبة المواطنين، استمرت وكالة الاستخبارات المركزية بعمليات مراقبة لآلاف المواطنين ضمن عملية اسمها CHAOS (أي فوضى)، تم تصميم هذا البرنامج لجمع المعلومات حول المعارضين لحرب فيتنام، الطلاب الناشطين، والمتعصبين الزنوج. كشفت هيئة التحقيق الكنسية (لجنة تحقيق مجلس الشيوخ يترأسها السيناتور Frank Church من مدينة Idaho) الكثير من هذه المفاسد، وتقلصت عمليات مراقبة الأمريكيين بشكل كبير. إلا أنه نتيجة أحداث الحادي عشر من أيلول عام 2001 المثيرة للجدل وانتقال المرسوم الوطني الأمريكي، المفصل في الفصل الثاني، يملك

المجتمع الاستخباراتي الآن قوى أكثر لإدارة عمليات التجسس ضد المواطنين. لا تزال عمليات اقتحام الحرية الشخصية للمواطنين موجودة، تحت ذريعة أن خسارة الحقوق الشخصية يعطي أماناً أكبر، وتسمح القوة المتزايدة للمجتمع الاستخباراتي بسوء معاملة المواطنين كما في الماضي.



كانت التحقيقات التي قامت بها لجنة التحقيق الكنسية واسعة وتضمنت قضايا مختلفة، محاولات اغتيال القادة الأجانب، الإطاحة بالحكومات، المراقبة المحلية وغير الشرعية التي تقوم بها وكالة الاستخبارات المركزية ومكتب التحقيقات الفدرالي. لمزيد من المعلومات انظر في الكتاب – في قلب وكالة الاستخبارات المركزية CIA – كشف أسرار وكالة التجسس الأقوى في العالم، للكاتب Ronald Kessler.

بالرغم من تأكيد وكالة الاستخبارات المركزية CIA ووكالة الأمن القومي NSA عدم قيامهما بعمليات التجسس الاقتصادي، إلا أن أي شخص على معرفة ضحلة بأعمال التجسس يعلم العكس. في عام 1995، طُرد خمسة من عملاء وكالة الاستخبارات المركزية العاملين في فرنسا بسبب قيامهم بأعمال التجسس الاقتصادي، مباشرة بعد تأكيد مدير الوكالة عن عدم تورطه بعمليات التجسس لصالح المؤسسات التجارية في أمريكا، وقد صدرت ادّعاءات بقيام وكالة الأمن القومي باعتراض رسائل بالفاكس ومكالمات هاتفية من وكالات أعمال أجنبية لإعطاء شركتي Boeing وRaytheon فائدة منافسة أثناء مناقصة الأسهم العالية القيمة.

تتفوق وكالات الاستخبارات الأمريكية في تقنيات المراقبة والإشراف، فهي ماهرة جداً بسرقة وتجميع المعلومات، وخاصة المعلومات الرقمية، هذه هي أحد أسباب استخدام تنظيم القاعدة طرائق اتصال قديمة غير إلكترونية بالإضافة إلى البريد الإلكتروني عالي المستوى وهواتف الأقمار الصناعية.

/جنبي

أمر هام لأية دولة في العالم أن تتفوق على منافسيها الأجانب، عرفت بلدان كثيرة هذا الأمر مثل الصين، كوريا الجنوبية، فرنسا، وإسرائيل واستخدمت خدماتها الاستخباراتية لتجميع المعلومات الاقتصادية بشكل سري ونقلها إلى مؤسساتها التجارية الضخمة الواقعة ضمن حدودها، وهم ليسوا بمهارة الولايات المتحدة في محاولة إخفاء ذلك.

جواسيس: مشروع RAHAB

في منتصف التسعينات، صدرت إشاعات حول حركة سرية حاسبية ومجتمعات أمنية لمخربين ألمان تدعمهم الحكومة متورطون في عملية اسمها السري RAHAB.

تشير كلمة RAHAB إلى مومس وجاسوسة ذكرت في الكتاب المقدس (عرفت باسم رحاب بائعة الهوى). وفقاً لمصادر متعددة، حوالي عام 1987، بدأت جماعة تنتمي لخدمة المخابرات الفدرالية الألمانية (BND) بتنفيذ عملية سرية مصممة لاختراق الشبكات وقواعد البيانات وسرقة معلومات اقتصادية وتقنية. لقد اخترقت هذه العملية افتراضياً حواسب في روسيا، الولايات المتحدة، اليابان، فرنسا، إيطاليا، والمملكة المتحدة. تضمنت بعض إنجازات هذه العملية تعريض شبكات شركة DuPont المشتركة للخطر بالإضافة إلى تخريب بروتوكول المناقلة الأمنية السريع للبنوك (هذا يعني أنه بإمكان المخرّب (Cracker) أن يتنصت على المناقلات المالية أو إنشاء مناقلات مزيفة لسحب الأموال من حساب إلى آخر).

تتوفر معلومات قليلة جداً عن مشروع RAHAB، لكن إذا كانت بعض المعلومات صحيحة فهو يمثل نظرة ممتعة للتجسس الأجنبي المدعوم حكومياً خلال الفترة الأولى لبدء استخدام الحواسب من قبل المؤسسات التجارية الضخمة.

تقوم الهيئة الاجتماعية الأمريكية للأمن الصناعي باستقصاءات حول حوادث التجسس الاقتصادي والصناعي المختبرة من قبل الأعمال الأمريكية من حين لآخر، خلال الاستقصاء الذي تم عام 1998، لاحظت البلدان الأجنبية التهديدات الكبيرة ومن هذه البلدان الصين، اليابان، فرنسا، المملكة المتحدة، كندا، المكسيك، روسيا، ألمانيا، كوريا الجنوبية، وإسرائيل.

لقد كانت هناك تفرقة كبيرة بين الأعداء والأصدقاء خلال الحرب الباردة، أما اليوم فإن الوضع قد اختلف. الغالبية العظمى من البلدان والتي تتجسس اقتصادياً ضد الولايات المتحدة هم الحلفاء السياسيون لها. فعلى سبيل المثال، وردت تقارير من خدمة المخابرات الفرنسية عن قيامها بالتنصت على الأحاديث الخاصة لركاب الدرجة الأولى ودرجة رجال الأعمال الراكبين على متن الخطوط الجوية الفرنسية، والتطفل على الحواسب المحمولة الخاصة بالزوار الأمريكيين من رجال الأعمال النازلين في الفنادق.

إذا كنت تسافر إلى الخارج لمتابعة أعمالك أو إذا كنت على اتصال بمواطنين أجانب مهتمين بشركتك ومنتجاتك، فعليك أن تكون حذراً من احتمال تطبيق التجسس الاقتصادي عليك.

المجرمون - مكاسب سيئة

بالرغم من أن أي جاسوس يخرج عن القانون فهو مجرم، يسعى "الجواسيس المجرمون" أن يصبحوا لصوص بيانات انتهازيين، فهم يمارسون التجسس على الحواسب بحثاً عن معلومات تساعدهم في الحصول على مكاسب غير شرعية أو فائدة شخصية لمصلحتهم. يقسم المجرمون إلى فئتين: المخرّبون (Crackers) والجريمة المنظمة (Organized Crime).

المخرّبون Crackers

المخرّبون هم الأشخاص الذين يقتحمون الحواسب بصورة غير قانونية. (نستخدم هنا الكلمة مخرّب (Cracker) بدلاً من الكلمة الأكثر انتشاراً (Hacker) وهي مصطلح مدرسي قديم لشخص ذكي وماهر تقنياً، لكن ليس من الضروري أبداً أن يخرج عن القانون). يهتم المخرّبون عادة بالمعلومات المالية، وخاصة أرقام بطاقات الاعتماد، الحسابات، والكلمات السرية التي تخوّلهم أن يخترقوا نظماً أخرى، قد يكون المخرّبون ماكرين فيحذفون الملفات أو ينشرون معلومات سرية. يمكن أن يكون المخرّبون غير محترفين (ذوي مهارات تقنية محدودة ويستخدمون أدوات وبرامج نصية مؤتمتة لاختراق الحواسب عن بعد)، أو أكثر احترافاً، وقد يكونوا من مدراء مزودي خدمة الإنترنت عديمي الضمير، وأخيراً محترفين ماهرين ممن هم على معرفة بجميع تعقيدات نظم التشغيل وبروتوكولات الشبكة. يسعى المخرّبون إلى رفع مستواهم، حيث من السهل جداً اعتراض محاولاتهم للتجسس وخاصة غير المحترفين.

الجريمة المنظمة Organized Crime

تشهد الجريمة المنظمة مستقبل التجسس الرقمي للحواسب، حيث تقدم لنا الحواسب جميع أنواع الأساليب لجني المال بطريقة غير قانونية، وأحدها هو إمكانية الوصول إلى الأجهزة الحاسبية دون إذن مسبق، ويقع اهتمام الجريمة المنظمة الأساسي على المعلومات المالية والبيانات الشخصية والتي يمكن استخدامها للخداع، والمعلومات المساعدة للتخطيط لجرائم أخرى سواء كانت مرتبطة بالحواسب أم لا. يمكننا تشبيه الجريمة المنظمة في كثير من الجوانب بتطبيق القانون وخاصة فيما يتعلق بتبني التقنيات الحديثة، لا يتمتع معظم المجرمين القدامى بمهارات تقنية جيدة، لكن الأجيال الجديدة والتي على علم أوسع بالتقنيات الرقمية، تحل محل القديم وبالتالي يزداد خطر الجريمة المنظمة المرتبطة بالتجسس على الحواسب. يوجد استثناء للرجال القدامى الذين يحتكرون المخدرات ويستخدمون تقنيات عالية جداً لحماية بنيتهم التحتية والتجسس على منافسيهم.

جواسيس: التجسس على الحواسب بالطريقة الكولومبية

أنفق اتحاد التجار الكولومبيين الذين قاموا باحتكار المخدرات بلايين الدولارات على تصميم بنى تحتية حاسبية معقدة، وقد قامت الشرطة الكولومبية، في عام 1994، بغارة على مجموعة من الأبنية الخاصة في مدينة Cali، ووجدوا هناك حاسباً مركزياً من الطراز IBM AS400 ويتصل به ستة أجهزة تنصت، كما تبلغ قيمة هذا الحاسب المركزي مليون ونصف المليون دولار أمريكي. تم شحن هذا الحاسب إلى الولايات المتحدة لإخضاعه للتحليل، بعد أن لُقب باسم "حاسب Santacruz" نسبة إلى الرئيس الاسمي للتجار المحتكرين Jose Santacruz Londono في مدينة Cali. إلا أن التقارير حول ما وجده التقنيون على الحاسب هي تقارير سرية، لكن معظم المعلومات قد تسربت مع مرور الوقت.

كان الحاسب يحتوي على قاعدة معطيات تضمنت أرقام الهواتف المنزلية وأرقام هواتف العمل لعملاء ودبلوماسيين من الولايات المتحدة المتمركزين في كولومبيا (ويشتبه بأنهم من عمال قوى القانون، الاستخبارات، والجيش). بالإضافة إلى ذلك، قامت مؤسسة الهاتف بتزويد التجار بسجلات كاملة للمكالمات الهاتفية على شكل أرقام الهواتف المرسلة والمستقبلة، ثم قامت القوة الاستخباراتية الخاصة بهؤلاء التجار باستخدام برنامج مصمم خصيصاً للمقارنة بين سجلات مؤسسة الهاتف مع القائمة الخاصة من العملاء والموظفين الذين يعملون في قوى القانون، الاستخبارات، والجيش لمعرفة أرقام الهواتف التي كانوا يتصلون بها أو الأرقام الواردة إليهم، ثم كانت العصابة تبحث عن الأسماء والعناوين الخاصة بهذه الأرقام، لتتشكل لديهم لائحة بالأشخاص الذين كانوا من المحتمل يبلغون عنهم.

لم يقم الموظفون في قوى القانون بأية تصريحات عما قد حدث للمخبرين الذين وجدهم الحاسب Santacruz، لكن إذا أخذنا بعين الاعتبار ميل المحتكرين إلى العنف، فمن المعقول جداً أن تعرض هؤلاء للتعذيب بهدف الحصول على المعلومات أو قتلوا في الحال. لا تتوفر أية مصادر لتقدير الخسارة البشرية الكامنة الناتجة عن عملية المحتكرين الحاسبية.

الوشاة - لكن للمصلحة العامة

سنعرض نوعاً آخر من الجواسيس والذي يعتبر من الجواسيس المفيدين (هذا يعتمد على من يقوم بالتجسس) وهو الجاسوس الواشي الذي يكشف عن الفساد والعمليات الخطرة على المصلحة العامة، بالتأكيد ما كان الوشاة موجودين لولا وجود وسائل الإعلام، والتي تمنحهم فرصة لسرد قصتهم، أو ينشغلون أحياناً بعمليات مراقبة مستقلة خاصة بهم.

نموذجياً، الوشاة هم دخلاء يملكون الوصول إلى أدلة لشيء سيئ يحصل، ويمكن أن يكونوا صحفيين يحضّرون قصة ما. يتميز الوشاة عادة بمهارات تقنية (إنترنت وحاسب) أكثر من

متوسطة يستخدمونها لصالحهم في الكشف عن الضرر. مع تطور الإنترنت، يملك الوشاة طريقة بسيطة لنشر المعلومات التي بحوزتهم والبقاء متخفين، واحدى هذه الطرق استخدام حسابات مؤقتة للبريد الإلكتروني ومرسلين مجهولين، ينشر الجاسوس المعلومات لطرف ثالث دون أي خوف من أن يتم كشفه. يمكن أن تنشر سجلات البريد الإلكتروني والرسائل الفورية المحرجة لشركة ما على شبكة الإنترنت بسرعة كبيرة.

إذا كنت تعمل لصالح شركة ما مثل شركة Enron، قد يتحلق حولك مجموعة من الجواسيس الكامنين، وقد لا يكون هذا بالأمر السيئ.

جواسيس: Cryptome.org

John Young أحد الأشخاص الذين يؤمنون بالخصوصية الفردية بقوة، وهو مهندس معماري من مدينة نيويورك، ويقوم بفضح أسرار الأشخاص الذين ينتهكون خصوصية الآخرين. يدير John الموقع Cryptome.org ويتضمن هذا الموقع معلومات مقتصرة على فئة قليلة من الناس تتعلق بوكالات الاستخبارات، الحكومة، الخصوصية، الرسائل المشفرة، المراقبة، والحرية.

قام Young بجمع كمية كبيرة من المعلومات السرية من مصادر مجهولة منذ عام 1996، تتضمن هذه المعلومات لوائح تفشي أسرار عملاء الاستخبارات الأجانب، لائحة بأسماء الزبائن لشركة تجهيزات للمراقبة تحتوي أسماء موظفي الحكومة، الجيش، وقوى تنفيذ القانون، نسخاً من برامج مراقبة غير محترمة، ومستندات متنوعة تابعة للحكومة من مصادر معروفة وسرية.

كسب الموقع Cryptome.org سمعة عالمية لنشره تفاصيل محرجة للأشخاص الذين يدرسون التجسس. يتصفح الموقع المحامون الخاصون، الجواسيس المختصون، المراسلون العاملون في مجال التحقيق والبحث، وبالإضافة إلى ذلك يقوم بزيارة الموقع رجال آليون مؤتمتون يقومون بجمع المعلومات يعملون لصالح وكالات استخبارات متنوعة ويقومون بتحميل معلومات جديدة للمحللين الحكوميين في محاولة لإيجاد شقوق أو استكشاف قطع من الأحجية الكبيرة للمخابرات.

الأصدقاء والعائلة - يا لهم من أصدقاء...

بالرغم من الاعتقاد الشائع أن التجسس يقتصر على الأعمال والحكومة، إلا أن الحقيقة تقول أن الحاسب المنزلي هو الأكثر عرضة للتجسس، لكن التهديد لا يأتي من المخربين الذين يستخدمون الاتصالات ذات الترددات الواسعة وإنما من الأصدقاء والعائلة.

قد يشك الأهل أحياناً أنك تقوم بشيء خاطئ ويبحثون عن الدليل، وقد يكون مجرد فضول منهم عن محتويات حاسبك ويبحثون عن المعلومات، وقد أضحت الحواسب جزءاً لا يتجزأ من حياتنا لذا فهي تسلط الضوء على أمور نريد الاحتفاظ بها لأنفسنا.

معظم الأحيان، تكون المعلومات والمهارات التقنية التي يتمتع بها الأصدقاء والعائلة ضئيلة بالمقارنة مع الأنواع الأخرى من الجواسيس، ويعتمدون على تصفح المجلدات واستخدام برامج تجارية مجانية رخيصة سهلة التثبيت.



تعتبر مسجلات المفاتيح (keyloggers) التهديد الأكبر فيما يتعلق بالتجسس ضمن العائلة. تتم مناقشة أدوات المراقبة هذه في الفصل الثامن.

شركاء السكن

يزداد عدد شركاء السكن والنزلاء في الولايات المتحدة بسرعة. لقد جرى الأمر في الماضي أن يكونوا شركاء السكن في الجامعة، لكن حالياً بسبب ضيق الأحوال الاقتصادية يقوم الأزواج القدامى الذين يملكون منزلاً باستقبال نزلاء ليتمكنوا من دفع الأجور المترتبة عليهم. فإذا كان بصحبتك رفيق بالسكن أو تقوم باستئجار غرفة أو شقة مع أحدهم، سيكون الحاسب غير المحمي هدفاً للتطفل.

مضبوط: من أفضل الأصدقاء؟

تشارك شاب يبلغ من العمر تسعة عشر عاماً يدعى Nicholas J. Suchyta بشقة سكنية مع فتاة من نفس السن في مدينة Bay في ولاية Michigan، وقد صرحت الفتاة عن صداقتها القوية مع Nicholas منذ المدرسة الابتدائية.

قام معارف الفتاة بإخبارها، في كانون الثاني (يناير) من عام 2002، أنهم شاهدوها في ملف فيديو مصور عبر الإنترنت مع صديقها الحميم البالغ من العمر ثمانية عشر عاماً في شقة Suchyta. قامت الفتاة بالبحث في حواسب Suchyta ووجدت صوراً عارية لنفسها، فتقدمت بشكوى للشرطة الذين وجدوا كاميرا ويب مخفية متصلة بحاسبها وأربعة ملفات للمراهقين في وضع حميمي.

في شهر أيار (مايو) من عام 2002، تم استدعاء Suchyta للمحكمة بتهمتي تثبيت أجهزة مراقبة، ونشر معلومات من هذه الأجهزة، وكان Suchyta قد وقع في مشكلة سابقاً بسبب

نشاطات تخريبية مزعومة أثناء عمله في مدرسة محلية، في تلك الأثناء قام Suchyta مع والديه بمقاضاة المدرسة بتهمة تشويه السمعة، التدخل في الخصوصية، إنزال عقوبة متعمدة نتيجتها أزمة نفسية،وإهمال جسيم، في النهاية لُقب Suchyta بلقب القرصان (Hacker).

الحواسب الثمينة

يبدو أن الثقة قد انعدمت في أيامنا هذه، يسعى الأزواج والزوجات الغيورين إلى حواسبهم الثمينة الحالية والسابقة في محاولة لإيجاد دليل لخيانة واقعية أو افتراضية.

لابد أن هذا الأمر مرتبط بالطريقة المجهولة والسهلة نسبياً لإنشاء علاقات عبر البريد الإلكتروني، الدردشة، والرسائل الفورية، أو ربما تأثير الإعلام عن طريق تشجيعه المتعة والاختبار بتغطيته الرهيبة للعلاقات عبر الإنترنت. وقد تمنح جميع هذه الإعلانات المعروضة على مواقع الويب لبرمجيات التجسس المصممة للقبض على شريكك، الناس شكوكاً حول علاقاتهم. مهما كان السبب فقد تحول التجسس باستخدام الحواسب الثمينة إلى عمل تجاري رائج.

الأهل

في بداية إطلاق خدمة الإنترنت، كان الأهل يقلقون حول كيفية إبعاد أطفالهم عن المواقع الموجهة للبالغين، أما الآن بالإضافة إلى مواقع الويب يتعرض الأطفال لغرف الدردشة، الرسائل الفورية، وحسابات البريد الإلكتروني الشخصية. يحث ترويج وسائل الإعلان حول مخاطر الإنترنت بعض الأهل ليقوموا بالتجسس على نشاطات أطفالهم الحاسبية. تتضمن برمجيات ترشيح الويب ميزات لمراقبة الدردشة والبريد الإلكتروني، تروج برمجيات تسجيل المفاتيح لمساعدة الأهل على اكتشاف ما يقوم به الأطفال أثناء تصفحهم الإنترنت.

مضبوط: وقت تفرقنا فيه لوحة المفاتيح

في عام 2001، انفصل Steven Paul Brown عن زوجته Patricia، لكن الانفصال لم يكن ودياً، حيث قام Brown بتثبيت برنامج مسجل مفاتيح تجاري يدعى eBlaster على حاسب زوجته السابقة. يقوم البرنامج بتسجيل بريدها الإلكتروني، تصفح الإنترنت، والدردشة، ثم إرسال نسخة من نشاطاتها إلى Brown. ارتكب Brown غلطة بذكره محتويات البريد الإلكتروني المتبادل بين زوجته السابقة وصديق، راودتها الشكوك وقامت وحدة النيابة العامة للجرائم التقنية عالية المستوى بإجراء التحقيقات.

اتهم Brown بتهمة تثبيت جهاز تنصت، التنصت، استخدام الحاسب لارتكاب جريمة، وامتلاك وصول دون إذن للحاسب (جميعها إهانات جنائية). يواجه Brown عقوبة قضاء مدة خمس سنوات في السجن ودفع غرامة بقيمة تسعة عشر ألف دولار أمريكي.

الأطفال

تعد نسبة كبيرة من الأشخاص البالغين غير ذكية كفاية فيما يتعلق بالحواسب، بالرغم من إمكانيتهم إنجاز مهام متعددة مثل استخدام برنامج تحرير النصوص، إرسال بريد إلكتروني، وتصفح الإنترنت، حيث لم يكونوا بحاجة إلى تطوير مهاراقم أكثر وخاصة فيما يتعلق بالأمن. ومن جانب آخر، نما الأطفال على الإنترنت وهم يجمعون معلومات هامة عن المهارات التقنية والتي تتجاوز تلك التي يتمتع بها الأبوان.

في الواقع، يطرح الأطفال تهديداً كبيراً كجواسيس مبتدئين، حيث يتم التحدث عن أدوات التجسس عبر البريد الإلكتروني وغرف الدردشة ومن ثم تحميلها فوراً من مواقع المخربين. يستطيع صبي ذكي عمره اثنا عشر عاماً أن ينصّب بسهولة برنامج مسجل المفاتيح على حاسب العائلة ويراقب نشاطات أفراد العائلة جميعهم. من السهل جداً فضح الخصوصية المتعلقة بالمناقلات المالية، الاتصالات بحواسب العمل، وتصفح الإنترنت والبريد الإلكتروني.

اكتشف مستوى جنون العظمة لديك

قال Sun Tzu أنه من أجل الخروج منتصراً من معركة عليك اكتشاف نفسك. لكن السؤال هو ما هو مدى الارتياب الذي يجب أن تتصف به مع كل هؤلاء الجواسيس المحتملين في العمل، في المترل، وعلى ما يبدو في كل مكان تتواجد به؟

أحد أقسام الإجابة هو أن تعرف نفسك (أو في حالة العمل، معرفة مؤسستك). فيما يلي اختبار سريع قد يساعدك في هذا الأمر. لا أهمية لعامل الوقت، لذا فكر جيداً في السؤال.

- ما هو الفرق بين تهديد محتمل لحاسبك أو شبكتك وتهديد لا أساس له؟ إذا كنت متحمساً لطائرات الهليكوبتر، سلطة الأمم المتحدة، والمكائد الحكومية التي لا أساس لها، أجب بالنفي.
- هل تستطيع أن ترتدي قناع الجاسوس وتستخدم أسلحته وتحاول أن تخترق نظام حاسبك الخاص؟ التفكير بعقل العدو هام جداً لتدرك نقاط ضعفك. سوف نطلب إليك من خلال هذا الكتاب أن تقوم بذلك.

- هل أنت مستعد أن تزود حاسبك بسياسات لضمان الأمن؟ سياسات الأمن هامة جداً، لكننا لن نغطيها في هذا الكتاب، إنما سنركز على وسائل التجسس والإجراءات المضادة.
- هل ستقوم بإتباع السياسات التي زودتها؟ إذا كنت تعتقد أن سياسات الأمن هي مجرد مضيعة للوقت وحمل ثقيل، أجب بالنفي.
- هل أنت مستعد للتزوّد مع بعض التردد لكن لزيادة الأمن؟ قاعدة الإبهام تقول كلما زاد الأمن مهما كان نوعه، نموذجياً تنقص الراحة وقابلية الاستعمال.

إذا أجبت بنعم لجميع الأسئلة، فلست متعلقاً بالتظنن، لكنك ببساطة مستعد وهذا ما يقلل من فرص التجسس عليك.

إذا أجبت بنعم لمعظم الأسئلة، قم باختبار الأسئلة التي نفيتها. قد تكون هناك بضع قضايا تمنعك من أن تكون مستعداً بالكامل لحماية حاسبك من خطر التجسس.

إذا نفيت معظم الأسئلة وكان هناك من يخطط للتجسس عليك، فبالتأكيد سوف ينجح. إذا كنت مهتماً بالأمر فحان الوقت أن تستعين بمساعدة خارجية.

حماية نفسك من التجسس عبر الحاسب هو أمر ما بين الجهل المنعم وارتداء قبعة معدنية لحماية دماغك من أشعة الراديو. عليك أن تجد التوازن الصائب.

خطر: الرموز الملونة

طور العقيد Jeff Cooper، وهو مدرب بارز للأسلحة النارية، رموزاً ملونة شائعة الاستخدام للإدراك والاستعداد وهي مبنية على خبرته في القوى البحرية. (نفذت حكومة الولايات المتحدة مؤخراً رموزاً ملونة مشابهة لأغراض الدفاع عن الوطن). يقسم Cooper نظامه إلى أربعة ألوان وهي:

- **الوضع أبيض.** وهو وضع نقص الإدراك التام للإدراك لأي تهديدات محتملة أو معلومات قد تقودك إلى الاعتقاد بوجود الخطر. يعيش معظم الناس طيلة حياتهم في هذا الوضع.
- **الوضع أصفر.** وهو إدراك خفيف، كحالتك عندما تقود بصورة دفاعية، فأنت مدرك لبيئتك والأشياء التي تبدو غير صحيحة. لا يكون الرمز الأصفر شاقاً، وبالتدريب عليك البقاء في هذا الوضع خلال ساعات اليقظة.
- **الوضع برتقالي.** وهو وضع الإدراك لتهديد كامن يجعلك تفكر وتخطط للتعامل مع هذا التهديد.
- **الوضع أحمر.** عندما تتعرف على تهديد حقيقي ومحدد وتتخذ الإجراءات لتتحكم بالموقف.

بالرغم من أن الرموز الملونة مصممة خصيصاً للدفاع عن النفس، فهي تصلح أيضاً كتوجه فكري لمنع التجسس الحاسبي. هل أنت مستعد للانتقال إلى حالة الوضع أصفر بالنسبة لحاسبك ومن ثم الصعود إلى مستويات أعلى إذا دعت الحاجة؟

تحليل الخطر 101

في بداية هذا الفصل طرحنا أحد أقوال Sun Tzu، "إذا عرفت عدوك وعرفت نفسك ليس عليك الخوف من مئات المعارك." هذا ما يتحدث عنه تحليل الخطر، ويتضمن ببساطة تعريف التهديدات الأكثر احتمالاً، تحليل نقاط الضعف، وتحديد الإجراءات المضادة التي يجب اتخاذها.

قبل أن نتابع من المهم جداً فهم معاني هذه المصطلحات المفتاحية الثلاثة.

- **التهديد.** التهديد هو شيء يمثّل خطراً. في كل مكان خلال هذا الكتاب، يمثّل الجواسيس التهديدات الرئيسة لأنهم يشكلون خطراً عن طريق قيامهم بنشر المعلومات على الحواسب.
- **نقطة الضعف.** نقطة الضعف هي حالة تسبب شيئاً ما قابلاً للهجوم. يبحث الجواسيس عن ثغرات في الأمن أو نقاط ضعف ليقوموا باستغلالها. فعلى سبيل المثال، قد يستغل جاسوس ما خطأ فيضان التخزين المؤقت المعروف في ملقم ويب ليكسب الوصول إلى الملفات ضمن الشبكة المشتركة.
- **الإجراء المضاد.** الإجراء المضاد هو نشاط يعوّض عن نشاط آخر. ببساطة، تمنع الإجراءات المضادة الاستغلال. أحد أمثلة الإجراء المضاد تثبيت برنامج ترميم لمنع هجوم فيضان التخزين المؤقت لملقم ويب.

لنطرح مثالاً تخيلياً لتحليل الخطر.

كانت عمتك Sara تحتفظ بوصفة لإعداد قالب شوكولا والتي ربحت إحدى الجوائز وقد كانت موضع حسد الجميع في البلدة، أعطتك العمة الوصفة عند وفاتها وطلبت منك ألا تكشف محتوياته لأحد. احتفظت بالوصفة على قرصك الصلب منذ ذلك الوقت، وبالرغم من الرشاوى والتهديدات التي تعرضت لها فلم تتشاركها مع أحد.

هل من الممكن أن يهتم الجواسيس الذين يعملون لصالح الحكومة بوصفة عمتك؟ لكن كل شيء ممكن، هل هذا يعني أنه عليك سحب تأميناتك على الحياة، استخدام حراس مسلحين، تثبيت ماسح لشبكية العين على حاسبك، وحماية مكتبك لمنع اعتراض الفيوض الكهرطيسية المتشردة من قبل رجال في شاحنات سوداء تحوي تجهيزات لاعتراض العواصف؟

بالرغم من إمكانية وجود عميل وغد مولع بالحلوى في وكالة الاستخبارات المركزية ، كان قد سمع عن وصفة عمتك، لكن هذا احتمال بعيد. لذلك اشطب العملية الاستخباراتية التي تدعمها الحكومة كتهديد محتمل، والآن بما أنه ليس عليك أن تقلق حول جميع هذه الأدوات والتجهيزات المعقدة المرتبطة بالتجسس المدعوم من قبل الحكومة، يمكنك طرد الحراس المسلحين وإعادة ماسح شبكية العين والواقي من العواصف. (بالطبع كل شيء ممكن أن يتغير إذا كان اسم عمتك الحقيقي هو Natasha وليس Sara، وكان ذراعها يحمل هذا الوشم المضحك السيف والترس وأحرف صغيرة تحته KGB).

قد يأتي التهديد الأكثر واقعية وخطراً من زوجة أخيك Christina، والتي كانت تسعى وراء الوصفة لسنوات عديدة. تحضر Christina وعائلتها سنوياً لعيد الشكر وعيد الميلاد، وعندما يضجر أطفالها تقوم بإرسالهم إلى المكتب ليلعبوا بألعاب على الحاسب. Billy الصغير بارع في الحواسب، وأثناء العشاء تتناقش معه حول الثغرات الأمنية لشركة Microsoft، كما أنك لم تثق بزوجة أخيك Christina يوماً وخاصة بعد الحادث البشع الذي يتعلق بآنية المائدة الفضية الخاصة بالعمة Sara. والآن ما هو التهديد برأيك، ما هي نقاط الضعف، وكيف يجب أن تتصرف؟

تهديد متوقع هو أن تدفع والدة Billy طفلها إلى التطفل على حاسبك ليتمكن من إيجاد الوصفة. تعلم أن Billy طفل بارع وخاصة فيما يتعلق بأنظمة التشغيل الخاصة بشركة Microsoft، لذا من الذكاء أن تضع الألعاب على نظام التشغيل Windows XP بينما الوصفة مشفرة بأمان باستخدام برنامج Blowfish على الحاسب المحمول الذي يعمل على النظام Linux، والمقفول في درج مكتبك في غرفة النوم. لقد قمت بتحديد نقطة الضعف وتقدمت بمجموعة من الإجراءات المضادة. (يحوي هذا الكتاب الكثير من نقاط الضعف والإجراءات المضادة الخاصة بالتجسس).

توجد جميع الأساليب للقيام بتحليل الخطر. يستخدم البعض نماذج رياضية، نسب قيم رقمية لأنواع مختلفة من الأخطار. نستمد الاحتمالات الإحصائية والتي تصنف ضمن المجموعة الكامنة من أنواع مختلفة من الخطر لتتمكن من اتخاذ قرارات أفضل لحماية نفسك من التهديدات المتنوعة.

تحليل الخطر بخمس خطوات

تحتاج مناقشة موضوع تحليل الخطر إلى الكثير من الوقت، وبما أن كتابنا يتحدث بشكل رئيسي عن تجسس الحواسب، سوف نعرض نموذجاً مكوناً من خمس خطوات لنساعدك على إنجاز تحليل خطر لتجسس الحواسب بشكل بسيط لكن فعال.

سوف نشرح كل خطوة على حدة ثم نطبقها على منظمتين خياليتين ذات مواقف مختلفة:

- المؤسسة التجارية e4bics، بدء تطوير تكنولوجيا متطورة للبروتوكول (VoIP) Voice over Internet Protocol
- No More Violence، منظمة مساندة ودعم من دون أرباح للنساء اللاتي يتعرضن للضرب.

معرفة ماذا لديك

في البداية، ماذا يحوي حاسبك من معلومات قيمة؟ قد تخزن هذه المعلومات إما على القرص الصلب (أو وسط تخزين آخر) أو تنتقل بين الحواسب إذا كنت تستخدم شبكة الإنترنت أو الشبكة المحلية (LAN). بالرغم من اعتقاد بعض علماء الاقتصاد أنه بإمكانك تخصيص قيمة مادية لجميع الأشياء، لكن هذا لا يعني أن القيمة المادية تعني المال في حالتنا هذه. قد تكون المعلومات ذات قيمة ملموسة (رقم بطاقة اعتماد أو أحد الأسرار التجارية)، وقد لا تملك هذه القيمة، قد تكون دليلاً إذا تم اكتشافه سيتم إرسالك إلى السجن أو تدمير علاقتك بأحد ما.

- أنهت المؤسسة التجارية e4bics عملها مؤخراً على تصميم ملقم اتصالات جديد خاص بالتقنية الصوتية المركزية والوسائط المتعددة، كما تنافس البرمجيات والأجهزة الخاصة بالمؤسسة بشكل مثير كل المنافسين من حيث الأداء والأسعار. تم التخطيط للبيان الرسمي التجاري على مدى ستة أشهر من الآن، لكن الإشاعات الصناعية تتنقل حول المنتج. سوف تكون المعلومات المتعلقة بالمنتج R&D، والتسويق قيّمة لأسباب جلية.
- بدأت منظمة No More Violence، بهدف تنسيق عملياتها، باستخدام قاعدة بيانات حاسبية لتعقب النساء اللاتي تدعمهم هذه المنظمة، أحد مهام المنظمة إيجاد أمكنة آمنة للسكن بشكل مؤقت لضحايا العنف المنزلي. تتضمن قاعدة البيانات أسماء النساء، العناوين، وبيانات شخصية أخرى، هذه المعلومات حساسة للغاية وقيّمة بصورة غير نقدية.

تحديد من قد يستهدف معلوماتك

والآن، فكر في من يرغب في الحصول على المعلومات القيّمة بنظرك. يتضمن القسم الأول من هذا الفصل لائحة طويلة من الأشخاص الذين يقومون بالتجسس، لذا يجب أن تكون قد تكونت لديك فكرة عن المشتبه بهم، وتذكر أن تصنف خصومك المحتملين أكثر من الخصوم المستحيلين البعيدين عن الشبهة، لكي تستطيع أن تركز كامل طاقتك على الأعمال التي من الممكن أن تحصل وليس الأعمال التي من البعيد أن تقع. حاول حصر مخيلتك وتأسيس ارتيابك جيداً.

- قد يرغب المنافسون الكبار أو الصغار، في حالة المؤسسة التجارية e4bics، الحصول على سبق صحفي هام حول التقنية الجديدة، وهذا يشمل الشركات من داخل الولايات المتحدة ومن خارجها. وقد اقترح العديد من الممثلين لمنافسين كبار على مدراء الشركة الشراكة على مشروعات مستقبلية، لكن تبدو الاتفاقات السرية لمصلحة المنافسين فقط.
- يرغب عدد من الرجال بإيجاد زوجاتهم السابقات بأسلوب عنيف ومزعج، بسبب أوامر الاعتقال الموجهة ضدهم من قبل الزوجات اللاتي تدعمهم المنظمة.

تقرير مدى شدة حاجتهم للمعلومات وكيف يستطيعون الحصول عليها

لنعتبر أنك حددت الخصوم المشتبه بهم الذين قد يتجسسون على بياناتك، ما هي شدة حاجتهم لها وكيف يحاولون الحصول عليها؟ عندما تجيب عن هذا السؤال، عليك أن تأخذ بعين الاعتبار اجراءاتك الأمنية ومدى فعاليتها في منع أو عرقلة الخصم. كما عليك اعتبار احتمالية وقوع مهاجمات متوقعة وليس نفيها. بالرغم من أهمية قضاء بعض الوقت في التفكير بجميع أنواع المهاجمات المحتملة، إلا أن الوقت أمر محدود، لذا من الأفضل التركيز أولاً على الأمور المرجحة.

- بسبب التأثير الكبير الذي قد يمتلكه المنتج الجديد الخاص بالمؤسسة التجارية e4bics على الصناعة، فمن الطبيعي أن يساورها القلق حول التجسس الاقتصادي. يملك المهندس الرئيسي في الشركة J.D.، المتخصص سابقاً بأعمال الاختراق لصالح القوى الجوية، لائحة طويلة بمختلف الأساليب التي قد يستخدمها خصوم الشركة للحصول على الأسرار التجارية وتتضمن عملية التفريغ، الهندسة الاجتماعية، اختراق المكاتب بعد ساعات طويلة، أو محاولة الدخول عبر ثغرة ما في الشبكة.
- مديرة الشبكة Sue في منظمة No more violence هي إحدى النساء اللاتي تلقين المساعدة من المنظمة ولديها معلومات حول الأمن. وقد قامت Sue أثناء حديثها مع مديرة مكتب المنظمة، بتسليط الضوء على إمكانية قيام أحدهم بسرقة ملفات قاعدة البيانات أو محتويات الحاسب بأكمله، يستطيع الجاسوس اختراق الحاسب عن بعد والوصول إلى قاعدة البيانات، مع العلم أن الحاسب المكتبي متصل بالإنترنت عن طريق كبل مودم ويعمل على نظام التشغيل Windows XP. تعلم مديرة مكتب المنظمة أن أحد الأزواج السابقين مدان بتهمة عملية سطو، اعتاد زوج آخر على اختراق المواقع التجارية للتسلية. قاعدة البيانات مصممة على برنامج Microsoft Access ومحمية باستخدام التشفير الداخلي الخاص بالبرنامج. تشير Sue إلى التشفير الضعيف لبرنامج Access وتتحدث عن تجربتها الشخصية في اكتشاف كلمة مرور ضائعة لقاعدة بيانات محمية باستخدام برنامج مجاني خاص بالمخربين في غضون ثواني.

التفكير بما قد يحصل عند نجاحهم في التجسس

تخيل الموقف الأسوأ الذي يمكن أن يقع. يخطط خصمك للحصول على معلومات حاسبك، ما هي العواقب المحتملة؟ حاول أن تكون دقيقاً جداً عند الإجابة عن هذا السؤال، وتطلع إلى الحاضر والمستقبل.

- في حالة المؤسسة التجارية e4bics، تعتمد آثار فضح المعلومات الخاصة بالشركة على ماهيتها. إذا كانت المعلومات المسروقة هي بيانات المبيعات، قد يستهدف الخصم الحسابات التي تقوم الشركة بتطويرها. إذا كشفت مخططات التسويق، يستطيع الخصم التخطيط لاستراتيجية معاكسة. إذا تمكن الخصم من الوصول إلى أسرار تصنيع المنتج R&D قد يتم إضعاف خطط المنافسة للشركة أو إزالتها كلياً. وكبداية بسيطة ستوضع أرزاق الشركة وموظفيها على المحك.
- الموقف الأسوأ الذي يمكن أن يقع في حالة منظمة No More Violence بسيط نسبياً. إذا وقعت قاعدة البيانات والتي تحوي أسماء وعناوين النساء بأيدٍ شريرة، سيكون أمن وحياة النساء في خطر منذ لحظة كشف المعلومات.

معرفة طرق الحماية والثمن

لقد قمت حتى الآن بمعرفة ما هو الشيء القيّم الذي تملكه، من قد يستهدفه، مدى قوة الحاجة إليه، كيفية إمكانية الحصول عليه، وماذا يحصل عند حدوث ذلك، والخطوة الأخيرة هي تحليل كل العوامل السابقة لوضع خطة حماية لهذا الشيء القيّم.

بما أن عامل المادة هام جداً، عليك اتخاذ بعض القرارات الواعية حول مستويات الأمن التي سوف تستخدمها لحماية المعلومات، لا تفكر بكمية الأموال التي ستدفعها لقاء منتج الأمان، عليك أن تتذكر دائماً بوجود علاقة متبادلة بين الأمن وقابلية الاستخدام، كلما ازداد مستوى الأمن ازدادت صعوبة إنجاز المهام اليومية للمستخدمين، وهذا يسبب تكلفة إضافية للشركة، أي تباطؤ بالنتائج الكمية والفعالة.

- يعلم المهندس .J.D أنه هناك الكثير من الاعتماد عليه من أجل الحفاظ على معلومات الشركة بأمان. حيث قام أولاً بتحليل الخطر وحدد نقاط الضعف التي قد يستغلها الجاسوس، ثم تقدم بمجموعة من الإجراءات المضادة المصممة للتغلب على نقاط الضعف، وأخيراً طور سياسة أمنية دقيقة تم توجيهها إلى قضايا الأمن المتعلقة بالحاسب والأمن الفيزيائي. لقد تفهّم المستثمرون والمدراء في الشركة أهمية حماية البيانات وأيدوا خطة وميزانية الأمن التي صممها .J.D. (في الحياة الواقعية تظهر في طريقك الكثير من التحديات

لإثبات أن خطر التجسس حقيقي وضرورة اتخاذ الإجراءات لمنعه، لكن بما أننا نناقش حالة افتراضية سوف تكون النهاية سعيدة).

- قررت مديرة مكتب منظمة No more violence، بعد التشاور مع Sue وشرطي ودود، تعزيز الأمن الفيزيائي بتركيب أقفال جديدة ونظام إنذار مراقب. تم شراء موجه NAT لحماية الحاسب من المتطفلين عبر الإنترنت (NAT هي اختصار إلى Network Address Translation ترجمة عنوان الشبكة، تزود وصولاً واضحاً إلى بقية عناوين IP للشبكة، عادة الإنترنت، من خلال حاسب ذي عبّارة واحدة (one gateway computer))، كما تم ترميم ثغرات الأمن لنظام التشغيل Windows XP، وأخيراً تم استخدام خدمة تشفير قوية، شائعة الاستخدام وآمنة تسمى Pretty Good Privacy (PGP) لحماية القاعدة. لا تتمتع المنظمة برصيد مالي كبير كما أن الموظفين لا يتمتعون بمهارات تقنية عالية، لذا كانت جميع الإجراءات الأمنية ذات سعر معقول، كما أنها غير ظاهرة لكي لا يتم العدول عن استخدامها.

تلخيص

لقد تكونت لديك فكرة أفضل عن كينونة عدوك (الجاسوس)، فيما إذا كانت لديك الأساليب المناسبة للقبض عليه، وكيفية الشروع بتخمين خطر التجسس الحاسبي.

في كل مكان خلال هذا الكتاب ستتعرف على عدد من الأساليب التي يستخدمها الجواسيس لنشر البيانات. عندما تقرأ عن هذه الأساليب تخيل أنك جاسوس وقدّر مدى فعالية هذه المهاجمات عليك، على عملك، على منظمتك. عليك دائماً الأخذ بعين الاعتبار فيما إذا كان الهجوم ممكن أو محتمل، حيث تكون جميع أساليب التجسس المعروضة ممكنة، لكن وضعك الشخصي الخاص سيجعلها أكثر أو أقل احتمالاً.

بما أنه يتم اكتشاف نقاط ضعف جديدة يومياً، مع استغراق بعضها وقتاً طويلاً لعرضها على الرأي العام، من الصعب امتلاك حاسب مؤمن بالكامل. هناك مقولة قديمة في مجال الأمن تقول أن الطريقة الوحيدة لحماية حاسب بشكل كامل هي قطع جميع أسلاكه، ملئه بالاسمنت، وطمره. ومع ذلك قد لا يكون آمناً تماماً.

تتلخص مهمتك بتقليص خطر التجسس الحاسبي قدر المستطاع. لا يمكنك التأكد أنه بمقدورك منع جاسوس من الوصول إلى معلومات أو دليل على حاسبك، لكن يمكنك جعل مهمته صعبة قدر الإمكان. سنأمل أن الثمن والجهد سيجعلانه يبحث عن أهداف أخرى.



التجسس والقانون

القوانين المتعلقة بالتجسس

علاوة على الوسائل والإجراءات المضادة المتعلقة بالتجسس الحاسبي، يجب الأخذ بعين الاعتبار الجانب الشرعي للموضوع. يعرض هذا الفصل خلاصة لبعض القوانين الأساسية وكيفية ارتباطها بالتنصت الحاسبي. قد تبدو لك بعض المواضيع غير مشوقة نسبياً بالمقارنة مع المواضيع التي تعلمك كيفية التجسس على الحواسب (والأهم كيفية منع الجواسيس من التجسس عليك)، لكن هذه المعلومات القانونية هامة لعدة أسباب:

- إذا كنت تظن أنك ضحية التجسس الحاسبي سواء على المستوى الشخصي أو مستوى العمل، فعليك طلب وكالة قانونية والتي تعمل مع مدعي لتحديد وجود قضية جنائية وكيفية التعامل معها، كما أن معرفتك الجيدة بالقوانين المرتبطة بالتجسس، وبشكل خاص تلك القوانين المرتبطة بجرائم الحاسب، يشجعك على التعامل مع المدعي العام (أو مدعي خاص يقتصر عمله على الدعاوى القضائية المدنية).
- إذا كنت تشك أن قوى القانون تمارس نشاط مراقبة الحاسب عليك، لأسباب حقيقية أو وهمية، فمن المفيد جداً فهم القوانين التي تحدد قواعد ارتباطهم والتي قد تساعدك على الدفاع عن نفسك، إذا تبين أنهم كانوا يتجسسون عليك بصورة غير شرعية.
- إذا كنت تعمل في قوى القانون، فمن الواضح جداً أنك تحتاج لمعرفة الأسلوب الصحيح لإجراء عملية مراقبة حاسبية. لا يفضل القضاة رجال القانون الذين يخالفون القواعد، وبالمقابل لا يفضل رجال القانون رؤية المجرمين أحراراً بسبب خطأ ما تم ارتكابه أثناء القيام بإجراء شرعي.

- إذا كنت جاسوساً أو كنت تطمح لتصبح جاسوساً، فانتبه، إذا تم القبض عليك توجد مجموعة من القوانين الجادة والتي قد تكلفك مبالغ مالية طائلة ووقتاً طويلاً خلف القضبان. إذا حكم عليك مدى الحياة بسبب جريمة ارتكبتها، فهذا هو الوقت المناسب لتتخذ الترتيبات المناسبة لتستخدم محامي دفاع يملك خبرة كافية بالقوانين التي ناقشناها، وذلك في حالة كشف مخططاتك المتعلقة بالتجسس.

نستشهد باختصار معروف للمجموعة الإخبارية USENET وهوIANAL (I am not a lawyer)، إذ لا يقوم هذا الفصل نصائح شرعية. فإذا تورطت بالتجسس الحاسبي على أي مستوى، سواء كنت الضحية أو الفاعل، فابحث عن مستشار قانوني، وقد يكون مستشارك المشترك، المدعي العام إذا كنت شرطياً، أو محامي خاص (لن تجد الكثير من المحامين في الصفحات الصفراء والذين يعلنون أن التجسس هو أحد اختصاصاتهم، لكن عليك البحث عن أحد ما على إطلاع بالتقنيات المعلوماتية والأسرار التجارية).

سوف نستعرض فيما يلي بعض القوانين الرئيسة التي تحظر عناصر التجسس الحاسبي، وكيفية تطبيقها على الجواسيس المدانين.

قرار تنظيم الجريمة الشامل وأمن الشارع عام 1968 (العنوان iii - قرار التنصت)

(Omnibus Crime Control and Safe Streets Act of 1968 (Title iii – Wiretap Act)

ما هي العلاقة بين تعزيز أمن الشارع والتجسس الحاسبي، ليتم سن قانون قبل ظهور واستعمال الحواسب عام 1968؟ لقد كان قرار أمن الشارع، بعد اغتيال الرؤساء Robert Kennedy و Martin Luther King الأصغر، يشكل لائحة قوانين قوية ضد الجرائم وتهدف إلى منع حيازة الأسلحة النارية للأشخاص غير الكفؤ لامتلاكها بناء على العمر، الخلفية الإجرامية، نقص التأهيل العقلي. الاستغراق في القرار (لنكون دقيقين في العنوان iii) هو قسم يتعلق بالتنصت على المكالمات الهاتفية، والاسم الشائع له العنوان iii أو قرار التنصت على المكالمات الهاتفية، والاسم الرسمي العنوان 18 لنظام الولايات المتحدة (United States Code U.S.C)، الأقسام 2510–2511.

تعني عملية التنصت على المكالمات الهاتفية وضع أداة تسجيل أو تنصت مخفية على خط الاتصال، وهذا يشمل بشكل خاص أجهزة الهاتف. يمنح القرار العنوان iii السلطة للجهات القانونية باستخدام أسلوب التنصت على المكالمات الهاتفية وتحدد معايير هذا الاستخدام، كما يفرض القرار أيضاً قيوداً على الذين يمارسون التنصت الإلكتروني، استطاع الجميع ممارسة التنصت على المكالمات الهاتفية قبل إصدار هذا القرار و لم تكن هناك قوانين تدين التنصت غير الشرعي.

في قضية تتعلق بالتنصت عام 1967، حكمت المحكمة العليا أن مكتب التحقيقات الفدرالي FBI يقوم باستخدام أجهزة إلكترونية للاستماع وتسجيل المكالمات الهاتفية دون حيازة رخصة للقيام بذلك، كل هذا أدى إلى انتهاك تفتيش غير معقول وتدابير الحجز على الممتلكات والمؤسسة من قبل التعديلات الدستورية الرابعة. لقد سمحت هذه القضية للمحكمة بفرصة للتصريح عن المعايير العامة للمراقبة الحكومية المسموح بها، والتي شكلت أساساً قوياً لصدور قرار العنوان iii.

كان الهدف الرئيسي من قرار العنوان iii هو الاعتراف بأن خصوصية المواطنين معرضة للخطر دون وجود سياسة واضحة فيما يخص التنصت على المكالمات الهاتفية، غير أن "يستخدم المجرمون المنظمون الاتصالات الشفهية والسلكية استخداماً واسعاً في نشاطاتهم الإجرامية." يزود القرار سماحيات لاعتراض هذه الاتصالات وحماية حقوق المواطنين.

يفصّل العنوان iii بشدة أهداف استخدام عملية التنصت على المكالمات الهاتفية، فعلى سبيل المثال لا يحق لمكتب التحقيقات الفدرالي أن يتنصت عليك بصورة قانونية بسبب عدم تسديد بطاقة وقوف السيارة. وفقاً للقرار الأصلي، يمكن استخدام التنصت على المكالمات الهاتفية في حالة الجرائم الخطيرة فقط مثل الرشوة، الخطف، السرقة، القتل، التزييف، الاحتيال، المخدرات، التآمر. (لكن مع ذلك عند صدور القرار العنوان iii، ازداد عدد الجرائم المشتبهة، والتي يسمح التنصت لها، من ست وعشرين جريمة إلى أكثر من مائة جريمة، ومن بينها جرائم خطيرة مثل الإدلاء بتصريحات كاذبة على طلبات القروض الطلابية).

يوجد نظام تدقيق وتوازن يعمل، ولا تستطيع الوكالات القانونية أن تجول في البلاد وتتنصت على من تريد، حيث يصدر القاضي أمراً بالتنصت قبل إمكانية البدء بالمراقبة القانونية. يجب استخدام طرق التنصت كطريقة أخيرة في القضية الإجرامية ويجب عرضها على القاضي وبيان استخدام جميع البدائل أثناء التحقيق قبل اللجوء إلى التنصت، كما يجب على الجهة القانونية توضيح وجود سبب محتمل، أي يجب أن يكون هناك دليل مقنع ليبرر للقاضي التنصت على المشتبه به، وبمعنى آخر لا تستطيع الجهات القانونية أن تروح جيئة وذهاباً إلى المحكمة لعلها تحصل على موافقة القاضي على القيام بالتنصت.

بالرغم من استخدام التنصت على أجهزة الهاتف، فإنه يطبق الآن على الاتصالات الإلكترونية، فعلى سبيل المثال إذا كانت الشرطة تحقق بقضية تتعلق بك، يجب عليهم الحصول على طلب التنصت ليتمكنوا من مراقبة بريدك الإلكتروني، وهذا يعني أيضاً إذا كنت جاسوساً وتستخدم برنامج تنصت sniffer بشكل سري للحصول على معلومات من شبكة ما بصورة غير قانونية، فأنت مذنب لانتهاك القوانين الفدرالية المتعلقة بالتنصت.

انتهاكات العنوان iii هي جريمة، تصل عقوبتها إلى قضاء مدة خمس سنوات في السجن ودفع غرامة تصل إلى عشرة آلاف دولار أمريكي.



للحصول على معلومات أكثر حول آراء وزارة العدل عن العنوان iii والتحقيقات الحاسبية، قم بزيارة الموقع:
www.usdoj.gov/criminal/cybercrime/usamarch2001_2.htm.

وسائل التجارة: لوائح الأرقام المطلوبة وأجهزة التعقب

قبل وقت طويل من ظهور الإنترنت، بدأت الجهات القانونية باستخدام لوائح الأرقام المطلوبة وأجهزة التعقب على خطوط الهاتف. لائحة الأرقام المطلوبة هي جهاز مراقبة يلتقط أرقام الهواتف للمكالمات الصادرة، ويحدد جهاز التعقب أرقام الهواتف الواردة (توافق خدمة كشف الرقم معايير جهاز التعقب). لا تتنصت هذه الأجهزة على المكالمات الفعلية، فقط أرقام الهواتف الصادرة والواردة.

بالرغم من أن التقنية تطبق عادة على الهواتف، لكن قوانين لوائح الأرقام المطلوبة وأجهزة التعقب تطبق حالياً على الاتصالات عبر الإنترنت (أصبح هذا رسمياً مع انتقال المرسوم الوطني الأمريكي USA Patriot Act). يتم إلحاق برنامج خاص، عند التنصت الحاسبي، إلى موجّه Router يقوم البرنامج بجمع معلومات مثل ترويسة البريد الإلكتروني (باستثناء الموضوع)، عناوين IP للمصدر والوجهة والمنافذ، ومحددات مواقع المعلومات لصفحات الويب، وبشكل عام أي شيء تناقلي *(أي لا يضم محتوى)* يكون متفقاً مع القواعد.

تحتاج لوائح الأرقام المطلوبة وأجهزة التعقب إلى إذن من المحكمة، لكن دون الحاجة إلى عرض سبب مقنع لاستخدام هذا الأسلوب من التحقيقات، كما في حال التنصت على المكالمات الهاتفية، مما يجعلها أسهل استعمالاً من قبل الجهات القانونية.

قرار مراقبة الاستخبارات الخارجية عام 1978

بالطبع لا يتمتع الجواسيس بكثير من الحقوق وخاصة الجواسيس الأجانب الذين يسعون إلى معرفة أسرار الدولة، لكن توجد عدة تدابير قانونية غير معروفة في الدستور الأمريكي للتعامل مع التجسس والأعمال الأخرى المرتكبة من قبل القوى الخارجية.

في عام 1978، أصدر الكونغرس الأمريكي قرار مراقبة الاستخبارات الخارجية (Foreign Intelligence Surveillance Act) أو FISA (العنوان 50 لنظام الولايات المتحدة

(United States Code U.S.C)، الأقسام 1811–1801). كانت الغاية من هذا القرار التفريق بين القوانين المتعلقة بالمراقبة الإجرامية كما هو محدد في قرار التنصت على المكالمات الهاتفية العنوان iii، وبين القوانين التي تطبقها الحكومة للمراقبة المتعلقة بالأمن المحلي وخاصة في حالات التجسس المرتكب من قبل قوى أجنبية. تم إصدار القرار FISA بالأساس لتوجيه القضايا المرتبطة بالمراقبة الإلكترونية، لكن تم توسيعه في التسعينات ليتضمن القيود الفيزيائية السرية أثناء إجراء التحقيقات واستخدام لوائح الأرقام المطلوبة وأجهزة التعقب.

يضبط القرار FISA عملية جمع "الاستخبارات الأجنبية"، وهي أية معلومات ترتبط بمقدرة الولايات المتحدة على حماية نفسها مما يلي:

- نشاطات عدائية محتملة من قوة خارجية أو عميل لصالح قوة خارجية.
- القيام بأعمال تخريبية من قبل عميل أو قوة خارجية.
- نشاطات استخباراتية خفية من قبل عميل أو قوة خارجية.

يمكن تطبيق قرار FISA بشكل أساسي، في حال وجود تورط أجنبي مرتبط بالدفاع الوطني، الأمن الوطني، أو إدارة الشؤون الخارجية للولايات المتحدة الأمريكية.

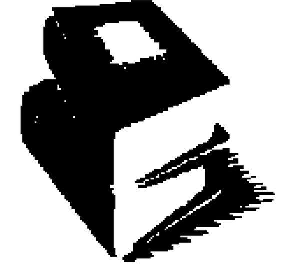
من أجل الحصول على مذكرة تفتيش، بناء على التعديلات الدستورية الرابعة، يجب وجود سبب محتمل على أنه تم ارتكاب الجريمة، بينما بموجب قرار FISA، يمكن تشريع نشاطات المراقبة عند وجود سبب محتمل أن شخصاً ما يمثل قوة أجنبية أو أنه عميل لقوة أجنبية، حتى عند عدم ارتكابه لأي جرم أو عدم التخطيط له، ولا يطبق القرار FISA على المواطنين الأجانب فقط، يمكن استهداف مواطن أمريكي بموجب هذا القرار طالما تواجد سبب محتمل للاعتقاد بتورط هذا الفرد في نشاطات تجسس لصالح قوة أجنبية.

بالرغم من أن الغاية من مراقبة القرار FISA هو تجميع الاستخبارات الخارجية، فقد حصل القرار على دليل يمكن استخدامه في المحاكمات الجنائية، إلا أنه يوجد متطلب تصغير minimization. تعني كلمة تصغير الحفاظ على المعلومات الخاصة بالاستخبارات الخارجية بشكل منفصل عن التحقيقات الجنائية الاعتيادية، وهذا أمر ضروري لأن القرار يمنح سلطات مراقبة موسعة. لكن في بعض الأوقات يحدث تداخل بين FISA والتحقيقات الجنائية، حيث يوجد ما يسمى "جدران ذات حاجب منخلي للمعلومات"، مثلاً يوجد ضابط غير متورط بالتحقيقات الجنائية يقوم بمراجعة معلومات FISA ومن ثم منح المحققين الجنائيين المعلومات المرتبطة بهم فقط.

أسست FISA محكمة خاصة، تدعى محكمة مراقبة الاستخبارات الخارجية (Foreign Intelligence Surveillance Court) أو FISC، وتتكون هذه المحكمة من سبعة قضاة

محكمة فدراليين عامين. تجتمع المحكمة FISC مرتين شهرياً وتراجع طلبات الحكومة من أجل المراقبة الإلكترونية لتحصل على معلومات الاستخبارات الأجنبية. (تجمع جميع الطلبات للحصول على رخصة من المحكمة FISC، بغض النظر عن الوكالة التي تطلبها بما فيها وكالة الاستخبارات المركزية CIA، من خلال وزارة العدل للمراجعة. يقوم المدعي العام بالتصديق على كل طلب للمحكمة).

تعتبر FISC محكمة سرية لأن جميع السجلات والملفات الخاصة بالقضايا مختومة وغير متاحة عادة حتى للأفراد الذين تعتمد مقاضاتهم على الدلائل التي تم الحصول عليها من ترخيصات FISA. كما توجد أيضاً محكمة استئناف خاصة بمراقبة الاستخبارات الخارجية، والتي تراجع وتحكم بشكل سري القضايا المثيرة للجدل والتي تصدر من المحكمة الدنيا FISC. (اجتمعت محكمة الاستئناف الخاصة بمراقبة الاستخبارات الخارجية لأول مرة في تاريخ القرار FISA عام 2002 لمراجعة طلب وزارة العدل لتغيير متطلب التصغير).



للحصول على النص الكامل للقرار FISA، اتبع الرابط:
www.law.cornell.edu/uscode/50/ch36.htm.

أساليب: CALEA

تعني كلمة CALEA قرار مساندة الاتصالات للجهات القانونية (Communications Assistance for Law Enforcement Act) الصادر عام 1994 (قانون عام 103-414، 47 وفق نظام الولايات المتحدة (United States Code U.S.C)، 1001-1010). بالرغم من أن هذا القرار لا يتعلق بشكل مباشر بالحاسب، لكنه جدير بالذكر لأنه يتضمن مراقبة إلكترونية.

لقد تطلب قرار التنصت على المكالمات الهاتفية، العنوان iii حوامل اتصالات عن بعد للتزود بأي دعم ضروري لإتمام عملية الاعتراض الإلكتروني. من ناحية ثانية لم يطرح السؤال فيما إذا كانت الشركات تلتزم بتصميم الشبكات الخاصة بها لكي لا تعيق اعتراضاً إلكترونياً قانونياً.

غير CALEA هذا الوضع بتعديل القوانين ECPA وطلب ضماناً لحوامل الاتصالات عن بعد بأن تجهيزاتها تراعي تقنيات المراقبة الإلكترونية القانونية. أتوقع أنه قد مرت عليك الرسالة التي تقول "متوافق مع نظام التشغيل Microsoft Windows"، أما بالنسبة لشركات الهاتف فيجب على جميع تجهيزات التبديل لديها أن تقول "متوافق مع التنصت الهاتفي".

يقوم قسم الاختبار في مكتب التحقيقات الفدرالي الذي يدعى (قسم تنفيذ CALEA)، (CALEA Implementation Section)، CIS، بتنفيذ قرار CALEA، تتلخص مهمته في "تزويد تجميع فعال، مراقبة، وأنظمة اتصالات تكتيكية لدعم أولويات التحقيق والاستخبارات. " بالإضافة

إلى الهواتف، توجد اقتراحات أن تتبنى FBI منظمات معايير أخرى وتدخل ميزات مراقبة ضمن خدمات DSL، Internet Protocol Telephony، Wireless Networking Protocols.

قرار CALEA ليس زهيد الثمن، حيث تم تقدير المصاريف التي ستنفقها شركات الاتصال عن بعد الأمريكية ما يتراوح بين نصف بليون دولار أمريكي إلى 2.7 بليون دولار أمريكي خلال مدة خمس سنوات. لذلك لا تتعجب أن الاتصال من حصالة الهاتف العمومية لم يعد يكلف ربع دولار فقط.

من الواضح أن صناعات الاتصالات عن بعد لا ترغب في تطبيق القرار CALEA، وقد سعت بكل طاقتها أن تتجنب تنفيذ مطالبها. وأخيراً في شهر أيار (مايو) من عام 2002، صدر أمر من هيئة الاتصالات الفدرالية إلى جميع شركات المواصلات البعيدة أن تطور أنظمتها إلى المواصفات التي طرحها مكتب التحقيقات الفدرالي FBI. لقد حاربت الصناعة والمجموعات الخاصة هذا الأمر من قبل FCC قبل ثلاث سنوات وسببوا له توقفاً تاماً في المحاكم. لكن حالياً لا يريد أحد أن يكون معادياً للحكومة وبالتالي لم تعد هناك أية حملات معارضة.

للحصول على مزيد من المعلومات عن CALEA، قم بزيارة الموقع www.askcalea.net، ولاستعراض القرار كاملاً افتح الصفحة www.law.cornell.edu/uscode/18/2522.html.

قرار خصوصية الاتصالات الإلكترونية عام 1986

وسّع الكونغرس عام 1986 بشكل مفاجئ نطاق العنوان iii المتعلق بقوانين التنصت الهاتفي بهدف دمج المحادثات الإلكترونية والتي تتضمن أجهزة تقسيم النواكر لأجهزة الراديو، البريد الإلكتروني، الهواتف الخلوية، حوامل الاتصالات الخاصة، وإرسال الحواسب. لُقّب القرار الموسع باسم قرار خصوصية الاتصالات الإلكترونية عام 1986 أو للاختصار ECPA (يلفظ "ekpa") للسرعة.

من التدابير الأساسية التي يتضمنها القرار ECPA هي:

- يحظر على جميع الأفراد، بما فيهم الحكومة والجهات القانونية، المراقبة غير القانونية للاتصالات الرقمية والتماثلية.
- تتم حماية خصوصية جميع أنواع الاتصالات الرقمية، وتتضمن إرسال النصوص والصور بين الأفراد.
- لا تقتصر خصوصية الاتصالات الرقمية على عدم اعتراض الرسائل المتبادلة فقط، بل حيازة وصول قانوني إلى الرسائل المخزنة على الحاسب.

قررت ECPA ثلاثة استثناءات للعنوان iii والتي لا تحتاج إلى موافقة المحكمة لاعتراض الاتصالات الإلكترونية وهي:

- يستطيع الفرد أو يجيز للحكومة بمراقبة الاتصالات على حاسبه إذا تعرض لهجوم ويتم استخدامه لأغراض غير قانونية. فعلى سبيل المثال، إذا اقتحم جاسوس ملقم وقام بإنشاء بريد إلكتروني للاتصال مع الجواسيس الآخرين، بإمكان مالك الملقم أن يسمح لجهات تنفيذ القانون أن تراقب البريد الإلكتروني بهدف تجميع المعلومات عن الجاسوس.
- إذا ظهرت رسالة عند محاولة الوصول إلى النظام تحذر جميع مستخدمي نظام الحاسب بأن الاستخدام خاص، وبدخول المستخدم إلى النظام هذا يعني أنه ستتم مراقبته، أي تمنح موافقة ضمنية لأي نشاطات مراقبة لهذا المستخدم.
- يعطي الاستثناء الأخير سماحيات لأي جهة خاصة أن تراقب نشاطات النظام لتمنع إساءة استخدامه عن طريق ضرر يصيبه، الاحتيال، أو سرقة الخدمات المتوفرة عليه، وليكون هذا الاستثناء مجدياً يجب تطبيق ذلك من قبل جهة خاصة وليس من قبل الحكومة. (في كثير من الحالات، طالما توافق الجهات الخاصة على عملية المراقبة فهي تعتبر قانونية).

لا يتوجه القرار ECPA إلى اعتراض اتصالات الزمن الحقيقي فقط، لكن قرار الاتصالات المخزنة أيضاً (Stored Communications Act) (العنوان ii من ECPA) يتضمن أيضاً تدابير للخصوصية فيما يتعلق بالاتصالات المخزنة. يمنع القرار فريقاً ثالثاً من امتلاك سلكاً مخزناً أو اتصالات إلكترونية مخزنة، مثل البريد الصوتي أو البريد الإلكتروني، دون إذن من المحكمة (تحتاج جهات تنفيذ القانون إلى إذن تفتيش للوصول إلى هذه الأنماط من البيانات، ويعتبر الحصول على مثل هذا الإذن أسهل من الحصول على أمر للتنصت الهاتفي). يتضمن القرار ECPA عقوبات جنائية ومدنية، وهذا يعتمد على التهمة.

توجد أيضاً استثناءات، كما في اعتراض الاتصالات الإلكترونية، والتي تسمح بالوصول إلى الاتصالات المخزنة دون الحصول على إذن من المحكمة. تتضمن هذه الاستثناءات ما يلي:

- **الموافقة الضمنية**. إذا أعلن مزود خدمة أو رئيس العمل عن تطبيق سياسة تراقب الاتصالات المخزنة، إذاً يمنح الموظفون أو المستخدمون موافقة ضمنية لتتم مراقبتهم.
- **الوصول إلى مزود الاتصالات**. يستعرض مزود الاتصالات الإلكترونية بشكل قانوني الاتصالات المخزنة على الخدمة التي يقدمها.

على المدى البعيد من مراقبة الموظفين، يعتقد بعض المحامون أن صياغة قرار الاتصالات المخزنة يعطي الرؤساء في العمل حقوقاً أكبر للوصول إلى الاتصالات المخزنة، مثل بريد إلكتروني مخزن مقابل اعتراض الرسائل الإلكترونية عند إرسالها.

مع أن القرار ECPA كان تقدمياً إلى الخلف في عام 1986 بالرغم من جميع التغيرات التكنولوجية على مدى ستة عشر عاماً، مثل هذا القرار التحديث الأخير المفيد لمقاييس خصوصية قوانين المراقبة الإلكترونية.



لمعلومات حول تدابير ECPA للتنصت الهاتفي، قم بزيارة الموقع www.law.cornell.edu/uscode/18/pich119.html. ولمزيد من التفاصيل عن قرار الاتصالات المخزنة، قم بزيارة الموقع:
www.law.cornell.edu/uscode/18/pich121.html.

أساليب: إحصائيات التنصت على المكالمات الهاتفية

إذا كنت من متابعي الأفلام أو التلفاز، فمن المحتمل أنك تعتقد أن التنصت على المكالمات الهاتفية هو أمر شائع جداً مثل ملفات MP3. لكن الحقيقة معاكسة تماماً، حيث وجد أقل من 1500 عملية تنصت هاتفية جنائية تم ترخيصها في الولايات المتحدة بكاملها.

يتطلب حزء من القرار العنوان iii تحضير تقرير سنوي، من قبل المكتب الإداري لمحاكم الولايات المتحدة، عن عدد عمليات التنصت الهاتفية الدولية والفدرالية والتي تم ترخيصها. تصدر هذه التقارير كل سنة في فصل الربيع وتتضمن معلومات مشوقة.

فعلى سبيل المثال، نستعرض فيما يلي الأعداد الكلية لعمليات التنصت الهاتفية التي تم ترخيصها خلال السنوات القليلة المنصرمة، تذّكر أن طلب التنصت يمكن أن يشمل الهاتف، أجهزة النداء Pager، أجهزة الفاكس، الحواسب، أو أي جهاز اتصال.

2001 – 1491

2000 – 1190

1999 – 1350

1998 – 1329

1997 – 1186

وافق القضاة على جميع طلبات التنصت عام 2001 (من النادر أن يقوم قاض برفض طلب تنصت)، ارتبط العدد الأكبر من عمليات التنصت الهاتفي، نسبة 78%، بالتحقيقات المرتبطة بالمخدرات.

لقد تم التنصت على أكثر من 23 مليون مكالمة هاتفية عام 2001، ونتج عنها 3683 اعتقالاً، وتمت إدانة شخص واحد من أصل كل خمسة أشخاص معتقلين، وتستخدم هذه النسبة من قبل مجموعات خاصة كدليل يثبت أن التنصت الهاتفي ليس بالوسيلة الفعالة لإجراء التحقيقات لأن البرهان الذي تقدمه غير كاف ليشارك في قرار الإدانة الذي يتخذه القاضي أو هيئة محلفين.

تمت مواجهة عمليات التشفير في ست عشرة عملية تنصت هاتفي تم ترخيصها في عام 2001، وجميعها من سلطات قضائية دولية أو محلية (من المثير في الأمر أن الفدراليين لم يقوموا بالإبلاغ عن أي حالات)، لم يتم الإبلاغ في أي حالة من هذه الحالات أن التشفير أعاق الحصول على نصوص الاتصالات غير المشفرة التي قام ضباط القانون باعتراضها. لكن هل يعني هذا أنه باستطاعة رجال الشرطة اختراق ما يسمى PGP أي (Pretty Good Privacy) وهذا أمر أشك به. على الأرجح كان هؤلاء الأشرار يستخدمون تشفيراً ضعيفاً، يستخدمون كلمات سر سهلة، أو يمارسون عادات أمنية سيئة، مثل كتابة كلمة سر على بطاقة عنوانها "Post-it®" ويلصقونها على شاشة الحاسب.

تشكل تقارير التنصت قراءات ممتعة جداً للجواسيس، وتتوفر على الرابط التالي www.uscourts.gov/wiretap.html.

قرار الاحتيال وإساءة الاستعمال الحاسبي عام 1986

تم سن قرار جهاز الوصول المزيف والاحتيال وإساءة الاستعمال الحاسبي (لنظام الولايات المتحدة (United States Code U.S.C 18) 18 1030 أو CFAA) في عام 1986 (وقد عزز قراراً قبله في عام 1984 للاحتيال وإساءة الاستعمال الحاسبي). إن هذا القرار هو أول قانون لجريمة الحاسب موجه بشكل خاص ضد المخربين Crackers، وقد خطط للقرار لينفذ ما يلي:

- جعل الوصول غير القانوني للحواسب الحكومية الفدرالية إجرامياً بسن هذا القرار.
- جعل الوصول غير القانوني للحواسب التابعة للمؤسسات المالية الكبيرة إجرامياً بسن هذا القرار.
- منح خدمة السلطة القضائية السرية للتحقيق في الجريمة الحاسبية (يتمتع حالياً مكتب التحقيقات الفدرالي FBI بالدور القيادي الفدرالي).

نشأ عن القرار الأصلي عدة إجراءات قانونية فقط، وأكثرها إثارة هي الإجراءات المطبقة ضد Robert Morris، وهو طالب متخرج من جامعة Cornell، وقد خرج برنامج الدودة التجريبي الخاص به عن السيطرة وانتشر بسرعة عبر الإنترنت. حكم Morris بموجب قرار CFAA إلى ثلاث سنوات من الاختبار، أربعمائة ساعة من الخدمات الاجتماعية، غرامة بقيمة 10050$، بالإضافة إلى تكاليف مراقبته.

تم تعديل القرار مرات كثيرة منذ عام 1986 ليتضمن عدداً من العوامل المختلفة للجريمة الحاسبية، فعلى سبيل المثال عدَّل قرار حماية البنية التحتية للمعلومات الوطنية عام

1996 (National Information Infrastructure Protection Act of 1996)، تعديلاً هاماً القرار CFAA، حيث تم توسيع مفهوم الحاسب المحمي (Protected Computer) ليشمل أي حاسب متصل بالإنترنت.

يحظر القرار CFAA ما يلي (قد تحدث أي من الانتهاكات التالية خلال سلسلة محاضرات التجسس الحاسبي):

- الوصول إلى "حاسب محمي" (وهو حاسب يستخدم للاتصالات، في الطريق بين الولايات، أو للتجارة الخارجية).
- الوصول إلى حاسب دون ترخيص وبالتالي نقل معلومات حكومية سرية.
- الابتزاز الحاسبي.
- الاحتيال الحاسبي.
- سرقة معلومات مالية.
- التجارة بكلمات المرور بهدف التأثير على التجارة بين الولايات أو على حاسب تابع للحكومة.
- إرسال شيفرة قد تسبب ضرراً لنظام حاسبي.

من وجهة نظر الإجراءات القانونية والقضاء، يشكل هذا القرار أحد أهم القوانين التي يستخدمها المدعي العام لإدانة الجواسيس والمخربين، تكلّف الإجراءات القانونية بموجب القرار CFAA مبلغ خمسة آلاف دولار أمريكي على الأقل (وقد يتضمن هذا المبلغ تكاليف الاستعادة). من جهة ثانية، قد يتم التنازل عن هذا المبلغ إذا تسبب هذا الحادث بضرر لأحد ما، استدعى عناية طبية، أو شكّل تهديداً للأمن الوطني. تتضمن الإدانة بموجب القرار CFAA عقوبة أقصاها قضاء مدة عشرين عاماً في السجن وغرامة تصل إلى قيمة 250000 $ دولار أمريكي.



للحصول على النص الكامل للقرار CFAA، اتبع الرابط:
www.law.cornell.edu/uscode/18/1030.html.

مضبوط: Konop ضد شركة Hawaiian Airlines

كان Robert Konop طياراً في شركة Hawaiian Airlines، وفي عام 1995 كانت الشركة تتفاوض حول عقود العمل الخاصة بالطيارين مع اتحاد الطيارين. شعر Konop بوجود بعض

الامتيازات غير العادلة الخاصة بالعمال في الصفقة، فقام ببناء موقع ويب محمي بكلمة مرور والتي منحها لبعض الموظفين فقط. عندما يستعرض أحد ما موقع الويب الخاص بالطيار Konop يتم عرض لائحة من الشروط التي يجب أن يوافق عليها المستخدم قبل أن يستطيع الدخول، كان أحد هذه الشروط عدم نشر معلومات الموقع إلى إدارة الشركة.

سمع نائب رئيس الشركة James Davis عن الموقع وأقنع طياراً يستخدم الموقع أن يسمح له باستخدام حسابه الخاص للدخول إلى الموقع. دخل Davis الموقع ثلاثة وأربعين مرة، مدعياً كونه الطيار ووافق على شروط الاتفاقية.

نقل Davis المعلومات عن الطيار Konop والمعلومات المتعلقة بالموقع إلى رئيس الشركة واتحاد الطيارين. اتصل ممثل الاتحاد بالطيار Konop وعبر عن استيائه فيما يتعلق بالموقع، دون الكشف عن مصدر هذه المعلومات. لعب Konop دور المحقق واستطاع استخدام سجلات النظام لتعقب الوصول وإرجاعه إلى Davis.

قام Konop أخيراً بمقاضاة الشركة على أسس دخول موظفين من الإدارة إلى الموقع دون ترخيص وانتهاك قرار التنصت وقوانين أخرى. رفضت المحكمة البدائية هذه المزاعم، لكن في شهر كانون الثاني (يناير) من عام 2001، أرجعت محكمة الاستئناف الدورية التاسعة هذه المزاعم، وأكدت أنه عند استعراض محتويات موقع ويب محمي بكلمة مرور دون الإذن من مالك الموقع، فهذا انتهاك واضح لقرار التنصت وقرار الاتصالات المخزنة.

ومع ذلك مع تغير مفاجئ للأحداث، سحبت المحكمة ذاتها أقوالها بعد مضي تسعة أشهر، وفي شهر آب (أغسطس) من عام 2002، قلبت القرار مصرحة أنه لم يتم انتهاك قرار التنصت لأنه يطبق على المعلومات التي يتم اعتراضها عند الإرسال، وغير المخزنة. التزمت المحكمة بالرأي القائل أن نشاطات شركة الخطوط الجوية من الممكن أن تكون قد انتهكت قرار الاتصالات المخزنة.

لمعلومات مفصلة حول هذه القضية والقرارات المختلفة، اتبع الرابط:
www.ca9.uscourts.gov/ca9/newopinions.nsf.

قرار التجسس الاقتصادي عام 1996

حتى عام 1996، لم يكن هناك أية قوانين فدرالية تتعامل بشكل خاص مع سرقة الأسرار التجارية. كان هناك بعض القوانين في عدة ولايات، لكن الحكومة الأمريكية لم تكن تملك شيئاً في سجلاتها لمقاضاة جواسيس الاقتصاد. تغير هذا الوضع بسن قرار التجسس الاقتصادي (العنوان 18 لنظام الولايات المتحدة (United States Code U.S.C)، الأقسام 1831–1839) أو للاختصار EEA.

يوجد تدبيران أساسيان للقرار وهما:

- سمح القرار لمكتب FBI أن يتولى التحقيقات في القضايا التي تشتبه فيها بتورط بعض الحكومات الأجنبية في سرقة معلومات تجارية خاصة بالأعمال الأمريكية. بالرغم من القيادة الدائمة لمكتب التحقيقات الفدرالي لدور مكافحة التجسس وخاصة فيما يتعلق بالتجسس الخارجي، إلا أنه حتى سنة 1996 تعامل المكتب مع قضايا الأمن الوطني فقط، والتي ليست طابع اقتصادي.
- تم إعادة تعريف المصطلحات "الممتلكات، السلع، أو البضائع" حسب القوانين الفدرالية المتعلقة بالممتلكات المسروقة لتتضمن معلومات الشركة الاقتصادية التابعة لها. انفتح هذا على تحقيقات وإجراءات قانونية فدرالية موسعة.

تتضمن انتهاكات القرار EEA بعض العقوبات الخطيرة – أقصاها قضاء مدة خمسة عشر عاماً وراء القضبان وغرامة أقصاها نصف مليون دولار أمريكي للأفراد، وما يصل إلى عشر ملايين دولار أمريكي لعمل أدين بدعمه لنشاطات التجسس. من الجدير بالملاحظة أن القرار EEA لا يطبق على نشاطات التجسس الاقتصادي الأجنبية فقط، بل على التجسس الذي تمارسه الشركات الأمريكية المنافسة ضد بعضها البعض.

إن الفدراليون مهتمون بهذا القانون على خلاف بعض القوانين الأخرى، ففي عام 1997 مثلاً، انتهك زوجان من ولاية فلوريدا القرار ECPA بالتنصت على مكالمات الهاتف الخلوي الخاصة بالمتكلم باسم المجلس التشريعي Newt Gingrich وتسجيلها على شريط، دفع كل منهما غرامة خمسمائة دولار أمريكي. لقد وقعت حوالي خمسة وثلاثون قضية، منذ صدور القرار EEA، تتضمن انتهاكات للقرار والكثير منها ذات عقوبات مجدية من غرامات وسجن.



يتعقب Mark Halligan وهو محام متخصص بالأعمال السرية التجارية، انتهاكات القرار EEA ويملك النص الكامل له بالإضافة إلى لائحة الاعتقالات والإدانات على الرابط التالي http://my.execpc.com/~mhallign/indict.html.

قوانين الولاية

بالرغم من أهمية القوانين الفدرالية، يقع تطبيق القانون معظم الوقت في الولايات وعلى المستوى المحلي. تتضمن معظم سجلات الولايات قوانين تشبه كثيراً القوانين الفدرالية المتعلقة بالجرائم الحاسبية، التنصت، وقوانين الخصوصية. (بعض هذه القوانين أكثر صرامة، مثل قرار الخصوصية في California، والذي يتضمن تدابير تفوق حمايات قرار التنصت الفدرالي العنوان iii).

قوانين الولاية محدودة النطاق، لأنها مصممة للتعامل مع أعمال إجرامية وشكاوى مدنية ضمن الحدود السياسية للولاية. أما عندما يتعلق الأمر بالتجسس الحاسبي الذي يمكن أن ينفذ من خارج الولاية، لا تملك حكومات الولايات التجهيزات الكافية لتعالج قضايا من خارج حدودها، كما لا تستطيع الوكالات القانونية الحصول على مذكرات تفتيش، أوامر المثول أمام المحكمة، أو إجراء اعتقالات خارج حدود الولاية، وفي هذه الحالة تدخل الوكالات الفدرالية على الخط.

إذا تم خرق قوانين الولاية والقوانين الفدرالية، يجتمع وكلاء الولاية العامون أو الوكلاء المحليون مع نظرائهم الأمريكيين من ولايات أخرى، ويقررون من سيلاحق الطرف المذنب في الجريمة.

تختلف القوانين بين ولاية وأخرى بشكل واضح في البنية والنص لكن ليس في الهدف. تجعل معظم القوانين الوصول أو الاستخدام المرفوض للحواسب وقواعد البيانات إجرامياً بسن القانون، وذلك باستخدام الحاسب كأداة احتيال، والقيام بأعمال معروفة ومنظورة لتخريب أجهزة الحاسب. إذا قمت ببعض أعمال البحث وعليك أخذ هذه القوانين بعين الاعتبار إذا كنت تخطط للقيام بعملية مراقبة أو تقبض على متنصت (مثلاً، في ولاية Virginia يحتاج طرف واحد فقط إلى الموافقة على اتصال مراقب، بينما في ولاية Maryland يجب أن تتم موافقة الطرفين على ذلك).



تغطية جميع القوانين المتعلقة بالتجسس الحاسبي هي خارج نطاق هذا الكتاب. يوجد لدى كل ولاية موقع ويب رسمي، ويتضمن معظمها إصدارات مباشرة قابلة للبحث لنظام الولاية، من بعض المصادر الأخرى للمعلومات حول القوانين الحكومية هو المؤتمر القومي للهيئات التشريعية في الولايات (www.ncsl.org/programs/lis/CIP/surveillance.htm)، والذي يتضمن ملخصاً عن قوانين الولاية المرتبطة بالمراقبة، ومعهد الأمن القومي (http://nsi.org/Library/Compsec/computerlaw/statelaws.html)، والذي يحوي موقعاً مع روابط لقوانين الجريمة الحاسبية.

خفايا المرسوم الوطني الأمريكي عام 2001

رداً على الهجمات المثيرة للجدل في الحادي عشر من أيلول (سبتمبر) عام 2001 على الولايات المتحدة الأمريكية، وقّع الرئيس Bush المرسوم الوطني الأمريكي (USAPA) في السادس والعشرين من تشرين الأول (أكتوبر) عام 2001. يطبق القضاء تعديلات على خمسة عشر قانوناً، بما فيها الكثير من القوانين الفدرالية التي تمت مناقشتها سابقاً. (توافه جاسوسية:

مصطلح الوطنية الأمريكية USA Patriot هو في الحقيقة كلمة مركبة لما يلي "وحدة وقوة أمريكا تتحلى بالتزود بالأدوات المناسبة المطلوبة لاعتراض وإعاقة الإرهاب. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and ("Obstruct Terrorism.

يتضمن المرسوم الوطني الأمريكي معنيين يتعلقان بالمراقبة الحاسبية وهما:

- منح الحكومة سلطات أوسع بكثير لإدارة المراقبة والتحقيقات، وهذا ما أقلق الكثير من مؤيدي القضية السريين.
- تطبيق عقوبات صارمة لبعض النشاطات التي قد ترتبط بالتجسس الحاسبي.

عبرت منظمات مختلفة مثل Democracy and Technology Center، Electronic Frontier Foundation، American Civil Liberties Union، و Electronic Privacy Information Center عن قلقها حول سرعة السياسيين في اتخاذ المرسوم من خلال الكونغرس ودون مراقبة فعلية بسبب الانفعالات بعد هذه الهجمات. يوجد تدبير ضمن المرسوم USAPA يسمى تدبير الغروب، والذي يدعو الكثير من التعديلات التي طبقت على المراقبة الإلكترونية أن تنتهي في نهاية عام 2005. ومن ناحية ثانية، من المستبعد أن تنتهي الحرب ضد الإرهاب خلال السنوات الثلاثة المقبلة، بسبب طبيعة النزاع القائم، لذلك سوف يتم تجديد هذه التعديلات.

بعد مضي سنة على توقيع لائحة القانون، أطلقت هيئة المجلس التشريعي للسلطة القضائية رداً لوزارة العدل DOJ (Department of Justice) بناء على طلبها لمعلومات حول كيفية تنفيذ المرسوم USAPA (الرسالة متوفرة على الرابط www.house.gov/judiciary/patriotresponses101702.pdf). أخفت وزارة العدل كمية كبيرة من المعلومات، ورفعت عدد من المنظمات دعاوى مستندة على قرار حرية المعلومات في محاولة لفضح بعض تفاصيل USAPA. سوف يظل المرسوم USAPA مثيراً للجدل، وهناك احتمال كبير عند وقوع هجمات مستقبلية أخرى على أمريكا أن يحدث تعديل آخر على القوانين المتعلقة بالمراقبة مسببة بذلك جدالاً أكبر.

نناقش في هذه الفقرة بعض التغييرات الأساسية التي أحدثها القرار USAPA على القوانين المرتبطة بالمراقبة الحاسبية.



يبلغ طول المرسوم USAPA أكثر من ثلاثمائة صفحة ويتضمن الكثير من التعديلات، للحصول على تحليل كامل للقرار، اتبع الرابط:
www.cdt.org/security/010911response.shtml.

قرارا التنصت والوصول إلى الاتصالات المخزنة

مع حلول مرسوم USAPA، تم تعديل قرار التنصت العنوان iii وقرار الوصول إلى الاتصالات المخزنة (تمت مناقشتهما سابقاً في هذا الفصل) بتعديلات هامة مرتبطة بالحواسب وتتضمن ما يلي:

- يجب أن تراعي شركات الأسلاك القوانين المحددة لعمليات الاعتراض والكشف للاتصالات من قبل شركات هاتف أخرى أو شركات مزود خدمة الإنترنت عند تقديمها خدمات الهاتف أو الإنترنت. سابقاً كانت شركات الأسلاك التي تزود خدمات الإنترنت تخضع لمجموعة أخرى من القوانين تختلف عن شركات الهاتف.
- يمكن الحصول على خدمة البريد الصوتي من خلال مذكرة تفتيش بدلاً من أمر صارم من قرار التنصت (ومع ذلك ما زالت الرسائل المخزنة على المجيب الآلي تتمتع بمستوى عالي من الحماية).
- تمت إضافة الإرهاب وانتهاك قرار الاحتيال وإساءة الاستعمال الحاسبي إلى الجرائم التي يتم التحقيق فيها من خلال التنصت.
- وضحت سلطة لوائح الأرقام المطلوبة وأجهزة التعقب أن يتم تطبيقها على حركة الإنترنت.
- تقع الحكومة حالياً تحت حماية من المسؤولية القانونية للاعتراضات دون ترخيص من قبل المخربين والمتعدين عند الطلب من مزود الإنترنت.
- تم تعديل قرار خصوصية الاتصالات الإلكترونية ECPA للسماح لمحكمة واحدة ضمن ولاية ما تملك سلطة قضائية بشأن جريمة ما أن تصدر مذكرة تفتيش للبيانات المخزنة مثل البريد الإلكتروني والتي تكون صالحة في أي منطقة من الولايات المتحدة (سابقاً كان القضاة يصدرون المذكرات ضمن حدود ولايتهم فقط).

قرار مراقبة الاستخبارات الخارجية

بما أن سبب صدور المرسوم USAPA هو تعزيز قدرة قوى القانون لتواجه الإرهاب الأجنبي، فمن المنطقي أن يتم تعديل القرار FISA، وتتضمن التغييرات ما يلي:

- **المراقبة المتعددة.** عادة عندما يتم منح الإذن للتنصت، يتم تحديد وسائل الاتصالات التي سوف تتم مراقبتها، مثل خط الهاتف أو الاتصال بالإنترنت. أما الآن بموجب USAPA تم توسيع القرار FISA للسماح بالمراقبة المتعددة لأهداف استخباراتية، وهذا يعني إمكانية صدور أمر واحد من المحكمة يمنح الإذن بمراقبة أي وسيلة اتصالات دون تحديد نوعها. لكن

هذا يعني أنه خلال تنفيذ عملية المراقبة من الممكن أن يتم التنصت على أشخاص آخرين يستخدمون أداة الاتصال بغض النظر فيما إذا كانوا متورطين بقضية التجسس أم لا. فعلى سبيل المثال، إذا كان المشتبه به يستخدم المكتبة العمومية للاتصال بالإنترنت، بإمكان رجال المخابرات أن يراقبوا نشاط الإنترنت للمكتبة بكاملها، كما تجدر الإشارة إلى تعديل آخر وهو إمكانية الاستخبارات منع المكتبة أو أي فريق ثالث يعلم بوقوع عملية المراقبة أن يكشف عن هذه العملية. تقدم جمعية المكتبات الأمريكية نصائح لأمناء المكتبات حول هذه القضية على الرابط www.ala.org/alaorg/oif/usapatriotact.html. لقد رفع مؤيدو السرية دعاوى جدية ضد التعديل الرابع بالنسبة لهذا التدبير.

- **لوائح الأرقام المطلوبة وأجهزة التعقب.** قبل أن تستطيع الحكومة استخدام وسائل لوائح الأرقام المطلوبة وأجهزة التعقب، يجب عليها بموجب القرار FISA أن تقدم دليلاً مقنعاً لمحكمة مراقبة الاستخبارات الخارجية بأن المستهدف من المراقبة هو عميل لصالح قوة أجنبية. تخلص المرسوم USAPA من هذا الشرط وتستطيع الحكومة الآن استخدام أدوات المراقبة لأي تحقيق كان بهدف جمع معلومات عن الاستخبارات الخارجية. لكن يوجد هناك تدبير يمنع استخدام أدوات المراقبة على المواطنين الأمريكيين استناداً على "أسس الأعمال المحمية بموجب التعديل الأول". أي على سبيل المثال، سوف يتم رفض طلب القرار FISA لاستخدام أدوات لوائح الأرقام المطلوبة وأجهزة التعقب، إذا كان المواطن المطلوب مراقبته مسلماً ولا يوجد أي دليل يدل على تورطه في أعمال التجسس.

- **قضاة أكثر لمحكمة الاستخبارات الخارجية FISC.** عين القرار خمسة قضاة إضافيين في محكمة الاستخبارات الخارجية للتزود بطاقة أكبر ومراقبة أفضل لطلبات المراقبة من قبل القرار FISA.

- **معايير المراقبة.** قبل صدور المرسوم USAPA، كان السبب الوحيد الذي يخول الحصول على إذن للمراقبة من قبل القرار FISA هو جمع معلومات عن أطراف خارجية، قام المرسوم USAPA بتغيير النص وتخفيض المعايير عن طريق الإعلان أنه عندما يكون سبب جمع معلومات عن أطراف خارجية هو "سبب وجيه" ستتم الموافقة على طلب المراقبة، لم يتم تحديد كلمة "وجيه" بدقة، ويبعث غموض هذه الكلمة على القلق.

قرار الاحتيال وإساءة الاستعمال الحاسبي

بالإضافة إلى التعديلات المتعلقة بالإرهاب بشكل واضح، أضاف المرسوم USAPA تعديلات لقرار الاحتيال وإساءة الاستعمال الحاسبي CFAA. شكك الكثير من مؤيدي الحقوق الإلكترونية

بهذه التغييرات، ووصفوها بمحاولة اتخذتها الحكومة لإضافة قوانين صارمة للجريمة الحاسبية بحجة التشريع ضد الإرهاب. وتتضمن التدابير الأساسية الجديدة المتعلقة بالتجسس الحاسبي ما يلي:

- تصنيف "المحاولة لارتكاب الجرم" بموجب القرار CFAA ليتم تطبيق نفس العقوبات كتنفيذ الجرم.
- تطبيق القرار CFAA خارج حدود الولايات المتحدة الأمريكية، إذا أثرت الأضرار الناتجة عن الجريمة على التجارة بين الولايات.
- زيادة العقوبات لأكثر من إدانة واحدة، بما فيها الإدانة في الولايات بموجب القوانين المشابهة للإدانات السابقة.
- زيادة العقوبات بسبب انتهاكات النظام، العقوبة القصوى هي عشر سنوات للجرم الأول وعشرون سنة للجرم الثاني.
- إعادة تعريف المصطلح "خسارة" ليتضمن الوقت المقضي لتقدير الأضرار، استرجاع البيانات، البرامج، النظم، أو المعلومات، الدخل الضائع، التكاليف المدفوعة، أو أضرار أخرى. (من السهل أن تصل قيمة الأضرار إلى خمسة آلاف دولار أمريكي أثناء القيام بالإجراءات القانونية).
- تصنيف الجريمة الحاسبية كعمل إرهابي إذا كانت تؤثر على الأمن القومي أو تسبب ضرراً ينشأ عنه إصابات جسدية، تسبب في تعطيل العناية الطبية، وتؤثر على الصحة العامة أو قضايا الأمان.

تضمنت الإصدارات السابقة للقرار تصنيف الاقتحامات الحاسبية منخفضة المستوى وتشويه مواقع الويب كجرائم إرهابية، لكن تمت إزالتها من الإصدار النهائي للقرار.

مضبوط: مفاسد القرار FISA

ترغب وزارة العدل أن يتم التشارك في المعلومات بين الجهات القانونية ووكالات الاستخبارات، لكن هذا الأمر يتعارض مع مفهوم التصغير minimization (تمت مناقشته سابقاً من خلال هذا الفصل)، تعني كلمة تصغير الحفاظ على المعلومات الخاصة بالاستخبارات الخارجية بشكل منفصل عن التحقيقات الجنائية الاعتيادية. أما سبب رغبة وزارة العدل بدمج عملية جمع المعلومات بين الجهات القانونية ووكالات الاستخبارات هو تسهيل حصول الجهات القانونية على إذن لإدارة عملية المراقبة إذا كانت أقوالهم هي أن العملية تنفذ ضد قوى أجنبية، مقابل القول

عن وجود مجرم في بستان شخص ما في الأحوال الاعتيادية. ومن جهة ثانية، عند دمج فرعي الاستخبارات مع بعضهما، سيكون من السهل جداً أن تنتهك قوى تنفيذ القانون القرار FISA وذلك بالتجسس على شخص غير متورط بأعمال إرهابية أو أعمال التجسس الخارجي.

أرادت وزارة العدل تقليص متطلب التصغير Minimization، لكن محكمة مراقبة الاستخبارات الخارجية FISC أعادت النظر في هذا الأمر، حيث تم الإعلان عن قرار المحكمة في شهر آب عام 2002، والذي تم تحضيره منذ شهر أيار.

صرح رئيس قضاة المحكمة FISC، قاضي المحكمة البدائية الأمريكية Royce Lamberth، عن قيام مكتب التحقيقات الفدرالي FBI بعدد مرعب من الأخطاء بحثاً واستخداماً لمذكرات الأمن القومي للتحقيقات في قضايا إرهابية منذ عام 2000. كما صرح قرار المحكمة "تضمنت التصريحات الحكومية الخاطئة والإغفالات في تطبيق القرار FISA وانتهاكات أوامر المحكمة، في كل طلب فعلياً، مشاركة للمعلومات والكشف غير القانوني للمحققين والمدعين الجنائيين." كان هذا من الأقوال القوية.

تقدم المدعي العام John Ashcroft بطلب لمشاركة أكبر للمعلومات لأسباب تتعلق بالأمن القومي إلى المحكمة العليا لمراجعة القرارات الخاصة لمراقبة الاستخبارات الخارجية على أمل تغيير قرار المحكمة FISC. أصدرت المحكمة العليا لمراجعة القرارات، في الثامن عشر من تشرين الثاني (يناير) عام 2002، رأيها لأول مرة مانحة وزارة العدل قوى جديدة لاستخدام التنصت في القضايا الجنائية، عكست المحكمة العليا قرار محكمة مراقبة الاستخبارات الخارجية التي قلصت هذه القوى من أجل الخصوصية الفردية للمواطنين.

تدابير أخرى

يتضمن المرسوم USAPA بعض التدابير الأخرى، يتعلق الكثير منها بالإرهاب ولا يرتبط بالتجسس الحاسبي، من الجدير بالذكر أن بعضاً من هذه البنود لا تتعلق بقوانين المراقبة الفدرالية. تتضمن هذه البنود ما يلي:

- يمكن نشر المعلومات الملتقطة من هيئة محلفين ضخمة ومن عملية تنصت بين مجموعة أكبر من مكاتب وضباط حكوميين.
- تم توسيع مجال أوامر المثول أمام المحكمة، ومن حق التحقيقات الوصول إلى المعلومات الخاصة بالمشتركين بخدمة الإنترنت، مثل طريقة الدفع، زمن ومدة الجلسات، وعناوين الشبكة المؤقتة.

- تستطيع مزودات خدمة الإنترنت كشف محتويات الرسائل الإلكترونية المخزنة ومعلومات أخرى عن المشترك، عند اقتناع المزود دون أي شك بأن حالة طارئة ترتبط بخطر فوري مثل خطر الموت أو إصابة جسدية خطيرة تهدد أحداً ما تحتاج لهذا الكشف.
- تم تحرير القوانين التي تمتثل لها الجهات القانونية لتتولى إدارة "البحوث السرية" خلال إجراء تحقيقات لأي جريمة فدرالية، بما فيها منح ملاحظة تأخير لأمر المذكرة للشخص الذي تطبق عليه. خلال معظم التحقيقات الجنائية يتم إعلام المواطن بوساطة نسخة من أمر التفتيش، أما عند عدم توفر المذكرة تسمح المحكمة بإعلام المشتبه به خلال وقت معقول، إذا كانت الملاحظة الفورية تعرّض التحقيق للخطر.

قوانين الولاية

بالرغم من أن USAPA هو مرسوم فدرالي، فقد غيرت بعض الولايات قوانينها الخاصة لتتماشى قوانين الحكومة الأمريكية. بدأت قرارات الولايات بالظهور مثل "الدفاع عن الوطن"، "مكافحة الإرهاب"، أو "أي اسم يثير ضجة على الساحة السياسية" بعد دخول USAPA ضمن القانون. تتبع هذه القوانين عادة القيادة الفدرالية في نشاطات المراقبة الموسعة والعقوبات المتزايدة لجرائم مختلفة.



للاطلاع على النص الكامل للمرسوم الوطني الأمريكي USAPA، اتبع الرابط .http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:%5D

حقائق حول تطبيق القانون

ترتبط فعالية القانون بشكل مباشر بمدى صرامة تطبيقه. بالرغم من عدم شرعية نشاطات التجسس الحاسبي بموجب قوانين عدة، لكن الحقيقة هي عدم وجود اجراءات قانونية ضد هذه النشاطات وخاصة إذا ما أخذ بعين الاعتبار مع الكمية المقدرة من التجسس الذي يحدث.

نعرض فيما يلي بعض الأسباب التي تجعل تطبيق القانون ضعيفاً:

- النظام المثقل قانونياً.
- العدد غير الكافي من ضباط القانون المؤهلين للتحقيق في التجسس الحاسبي بصورة مناسبة.
- صعوبة كشف أعمال التنصت الحاسبي.

- نقص الأدلة الكافية.
- عدم رغبة الضحايا بالتبليغ عن التجسس بسبب العلاقات العامة السلبية وانعدام ثقة حامل الأسهم.
- تكريس الانتباه والموارد للحرب ضد الإرهاب على حساب جرائم أخرى والتي قد تتضمن التجسس الحاسبي.

لا تظن أن التجسس آمن مثل أمان قيادة سيارة بسرعة 60 ميل في الثانية في منطقة يسمح فيها القيادة حتى 55 ميل في الثانية، ومن جهة ثانية زادت أعداد القضايا على المستوى المحلي ومستوى الولايات المتعلقة بالتنصت الحاسبي. مع أنها تبدو قليلة جداً بالمقارنة مع مشاهد التجسس التي تتميز بها الحكومة والأعمال البارزة والعالية المستوى، فهم يقومون بتعيين متقدمين قانونيين والتعامل مع مدعين يعملون مع هذا النوع من الجرائم. اقترن المدعون وقوى القانون الحاسبية الذكية بالصرامة عند وقوع الجرائم بشكل متزايد، حيث بدأت الدوافع السياسية تتوق إلى مكافحة الجريمة الحاسبية.

إذا كنت تخطط لأي نوع من التنصت، فعليك التفكير فيما إذا تم اعتبار أفعالك مرتبطة بالإرهاب بشكل أو بآخر، حتى في أبعد الظروف، حيث يتم التدقيق على النشاطات اليومية والتي تحتل مكاناً هاماً في أي تحقيق. فعلى سبيل المثال، خلال صيف عام 2002، طالبت التحقيقات الفدرالية بسجلات الانتساب من منظمات الغوص وسجلات الزبائن من محلات الغوص التجارية لأي شخص اجتاز تدريبات الغوص تحت الماء. كان السبب وراء هذا هو إمكانية الغواصين أن يفجروا السفن في المرافئ الأمريكية، تم إبعاد هذه النظرية من قبل كثير من الغواصين ومحترفين أمنيين.

إجراءات مضادة: مكتب تحقيقات فدرالي أكثر ودية ولطافة

يدرك مكتب التحقيقات الفدرالي أن الجريمة الإلكترونية بما فيها التجسس الحاسبي هي مشكلة متزايدة. صرح مدير مكتب التحقيقات الفدرالي Robert Mueller في خطاب له في شهر تشرين الأول (أكتوبر) عام 2002 للحاضرين من مجموعة تجارية صناعية، أنه يتم الإبلاغ بشكل تقديري عن ثلث الاقتحامات الحاسبية فقط للوكالة. مع العلم أن الكثير من المؤسسات التجارية تتجنب قوى القانون بسبب رد الفعل العام السلبي عند الكشف عن الاقتحام، تابع Mueller ليطمئن الصناعة والصناعيين وقال:

"دعوني أطلعكم ما الذي لن يحدث إذا قمتم بالتبليغ عن جريمة إلكترونية أو اقتحام. لن نحيط البناء بعملائنا الذين يرتدون ستراً ذات واق معدني ومحفور عليها من الخلف .F.B.I، نحن نقدر قيمة الاقتراب المتخفي في هذه المسائل، مهمتنا هي مساعدة الشركة الضحية وليس مقاضاتها. سوف يأتي عملائنا بملابس غير رسمية، وربما بحجة متعاقدين أو مستشارين، إذا دعت الحاجة.

لن نقوم بعقد مؤتمر صحفي أو ننشر خبراً صحفياً، لا نقوم بهذا تجاه القضايا المعلقة، أما فيما يخص الثغرات فهي ممنوعة منعاً باتاً، وإذا وقعت سيعالج المسؤول عنها أمره معي شخصياً.

لن نقوم بالاستيلاء على نظامك أو ربط أجهزة خارجية إلى شبكتك.

كما لن نقوم بقراءة ملفاتك لدراسة خطتك للامتثال للأوامر، أؤكد لكم نحن غير مهتمون بملفاتكم."

تسعى FBI إلى تشجيع الصناعة للتبليغ عن الحوادث، وليتحقق هذا عليها أن تكسب ثقة الصناعة، وهذا ما سنراه قريباً.

المحكمة المدنية مقابل المحكمة الجنائية

لقد جرى الحديث في هذا الفصل حتى الآن عن القانون الجنائي، لكن عندما يتعلق الأمر بالتجسس المشترك إضافة إلى الإجراءات الجنائية، يوجد احتمال أن ينتهي أمر عملية تجسس مكشوفة إلى المحكمة المدنية.

تحدث الإجراءات المدنية عندما يتهم شخص أو وجود قانوني ما (شركة، منظمة، أو حكومة) شخصاً أو وجوداً قانونياً آخر بالتسبب بضرر وتسعى إلى الحصول على تعويض من المحكمة. يستخدم كل طرف محامين خاصين به، ويحل القاضي أو هيئة المحلفين القضية. فعلى سبيل المثال، إذا تم القبض على جاسوس يعمل نيابة عن منافس ما محاولاً أن يسترجع دخلاً مفقوداً بسبب أعمال التجسس.

يوجد اختلافان هامان بين المحكمة المدنية والجنائية:

- **العقوبات.** تفرض عقوبات سجن، غرامات نقدية، أو كليهما على الفريق المذنب في المحكمة الجنائية، بينما تتضمن عقوبات المحكمة المدنية الغرامات النقدية فقط.
- **الإثبات مطلوب.** في القضايا الجنائية، يجب على المدعين أن يثبتوا دون أدنى شك أن الفريق مذنب، أي يجب أن يوجد دليل كاف ليعتقد أي إنسان عادي أنه لا يوجد أي شك أن هذا الشخص مذنب. أما المحاكم المدنية فهي تتمتع بمعايير أقل بالنسبة للدليل المطلوب وتسمى "رجحان الدليل"، هذا يعني وجود الحاجة لدليل كاف لإدانة الشخص أكثر من

عدم وجوده. من الأمثلة الشهيرة وغير المرتبطة بالتجسس عن الحاجة للإثبات المطلوب هي قضية *O.J. Simpson، حيث لم تتم إدانة Simpson من قبل هيئة محلفين في المحاكمة الجنائية التي جرت عام 1995 بسبب عدم قدرة القضاء إثبات جرمه دون شكوك معقولة، لكن من جهة ثانية خلال محاكمته المدنية التي جرت عام 1997 اعتقدت هيئة المحلفين بوجود أدلة كافية لجعل Simpson مسؤولا قانونيا عن وفاة Ronald Goldman و Nicole Brown Simpson، ومنحوا تعويضاً بقيمة 8.5 مليون دولار أمريكي لعائلات المغدورين.

من الجدير بالذكر أيضاً، أن المحكمة تستطيع أن تصدر أوامر الحجز على الممتلكات في القضايا المدنية. مثلاً إذا اعتقد القاضي أن الشركة المتهَمة (الفريق المطالب بالتعويض) تملك دليلاً يثبت التجسس على ملقماتها المشتركة، فبإمكانه أن يصدر أمراً للحجز على الملقمات، ويتم تنفيذ الأمر من قبل ضباط القانون وممثلين من جانب الادعاء (الفريق الساعي للحصول على تعويض). كما يمكن أن يتضمن أمر الحجز المعلومات، مثلاً تستطيع مؤسسة تجارية أن ترفع دعوى باسم John Doe ضد شخص مجهول ومن ثم تجبر مزود خدمة الإنترنت أن يظهر بيانات المشتركين التي قد تكون مرتبطة بالدعوى.

مضبوط: غارات على موقع Amazon

تلقى بائع الكتب عبر الإنترنت Alibris اتهامات فدرالية، في شهر تشرين الأول عام 1999، لقيامه بالتنصت على بريد إلكتروني مرسل من قبل الموقع Amazon.com وحيازته كلمات مرور حاسبية مرفوضة. واجهت الشركة عشر اتهامات بانتهاك القرار ECPA واتهاماً واحداً لحيازة مرفوضة لكلمات المرور مع نية الاحتيال. وصلت عقوبة كل تهمة من التهم السابقة إلى مبلغ 250000 دولار أمريكي، لكن Alibris استطاع أن يدفع غرامة واحدة فقط بهذه القيمة.

كان رئيس الشركة السابق، الذي أوقف عمله تحت اسم Interloc Inc، بائعاً للكتب عبر الإنترنت وقد كان يدير عملاً مساعداً كمزود لخدمة الإنترنت تحت اسم Valinet. اعترضت شركة Interloc وخزنت آلاف الرسائل الإلكترونية، خلال عام 1998، المرسلة من موقع Amazon إلى زبائنه الذين كانوا يستخدمون خدمات مزود خدمة الإنترنت، والكثير منهم كانوا بائعي كتب. بالرغم من عدم كشف أي معلومات خاصة أو مالية، زعم المدعون أن حدوث هذه الاعتراضات كانت لمصلحة عمل بائع الكتب Alibris. (كما صرح المدعون أيضاً عن احتفاظ شركة Interloc بنسخ مرفوضة من ملفات كلمات مرور سرية ولوائح الزبائن الخاصة بمزودات خدمة الإنترنت المنافسة).

* O.J.Simpson هو لاعب كرة قدم أمريكي مشهور، اتهم بقتل زوجته وعشيقها، لكنه نجا بفعلته حدثت هذه الجريمة عام 1993، ومنذ ذلك الوقت يضرب المثل بهذه القضية عن الأشخاص الذين يرتكبون جرماً ولا يتلقون العقاب، كما تمثل هذه القضية العنف المنزلي في أمريكا.

بسبب عدم تضرر Amazon بشكل كبير، لم تتم إضافة أي تهم جنائية أو مدنية ضد Alibris. صرح رئيس شركة Alibris، Martin Manley،"نحن شركة مختلفة ذات عمل مختلف حالياً، وكان الوقت مناسباً جداً للقيام بهذا التغيير." لا يزال Alibris يعمل حالياً ويعتبر من قادة المبيعات الإلكترونية للكتب المستعملة والنادرة.

المدراء والموظفون - تجسس شرعي

لا يستطيع المدير، بموجب القرار ECPA، أن يقوم بمراقبة المكالمات الهاتفية للموظف أو بريده الإلكتروني عندما يتوقع الموظفون وجود نسبة معقولة من الخصوصية — مثال على وجود نسبة معقولة من الخصوصية هي قاعات الاستراحة بدون كاميرات مراقبة. من جهة ثانية، يسمح القرار ECPA للمدير أن يتنصت على الموظفين إذا تم تنبيه الموظفين إلى ذلك مسبقاً أو إذا اعتقد المدير أن مصالح الشركة في خطر، توجد إعفاءات واسعة جداً لذلك إذا كنت موظفاً فمن الأفضل الافتراض أن أي شيء تفعله على حاسبك هو مراقب. لكن توجد استثناءات وهي:

- **موظفو الحكومة.** تمنح تعديلات الدستور الأولى والرابعة والرابعة عشر الموظفين الحكوميين حقوقاً وصلاحيات لا يملكها موظفو القطاع الخاص. فعلى سبيل المثال، يتوجب على المدراء الفدراليين، الحكوميين، والمحليين احترام حق حرية الكلام لموظفيهم ولا يستطيعون ممارسة عمليات تفتيش وحجز على ممتلكات الموظفين.
- **موظفو النقابات.** يتم تطبيق قرار العلاقات العمالية الوطنية (National Labor Relations Act) NLRA في مكان عمل منظم أو يتم تنظيمه. وتستطيع اتفاقية المفاوضات حول أجور وشروط العمل بين النقابة وأرباب العمل أن تحد من حق المدير اعتراض اتصالات الموظفين، حتى لو سمح القرار العنوان iii أو قانون الولاية بالتنصت. كما بإمكان القرار NLRA أن يحد من حق المدير اعتراض اتصالات الموظفين إذا كان هذا الاعتراض يؤثر على "حق التنظيم الذاتي" أو "النشاطات الموحدة".

بالرغم من عدم وجود قوانين فدرالية خاصة بمكان العمل حالياً، تحقق بمساعدة محامي أنك لا تتجاوز حدودك القانونية إذا كنت تخطط لمراقبة الموظفين العاملين لديك. وسعّت بعض الولايات قوانين السرية مثل قرار السرية في ولاية California. من المنطقي حالياً الاستمرار بتشريع قوانين تتعلق بمكان العمل بسبب مطالبة الشعب المتزايدة للسرية.

بالرغم من أن القوانين تقف بصف المدير، إلا أنه المدير الفطن يتخذ بعض الخطوات الاحترازية لتقليص احتمال وقوع دعوى قضائية بموجب قوانين السرية. خذ بعين الاعتبار ثلاث تقنيات بسيطة غير مكلفة تجنبك جميع أنواع المتاعب وهي:

- **استخدام موافقة ضمنية.** استخدم شعاراً لتسجيل الدخول، شاشة برمجية "مزعجة" (تتوفر في كثير من البرامج لمراقبة لوحة المفاتيح)، أو أي أسلوب واضح آخر لإعلام الموظفين عن مراقبة البريد الإلكتروني، استعراض الإنترنت، أو أي نوع آخر من الاتصالات.
- **استخدام موافقة صريحة.** قم بإنشاء وتوزيع اتفاقيات بين الموظفين أو أي مستندات أخرى حيث يوافق الموظفون صراحة على عملية المراقبة.
- **استخدام توقيع للبريد الإلكتروني.** قم بإلحاق فقرة مختصرة إلى نهاية جميع الرسائل الصادرة والتي تنص أن جميع الرسائل تقع تحت المراقبة. بالرغم من أن هذا العمل يبدو زائداً، لكنه يُعلم أي شخص يرد على رسالة صادرة أن الرسائل المتبادلة ليست شخصية.

تشكل سياسة المراقبة المكشوفة رادعاً ضد إساءة استخدام الموظفين للموارد، إضافة إلى كونها حماية للمدير من الدعاوى القضائية، فإذا علم الموظفون بمراقبة مكان العمل فستقل محاولاتهم لسرقة بيانات الشركة.

قضايا قانونية مع أفراد العائلة

أبلغت اللجنة الوطنية لمراجعة القوانين الفدرالية وقوانين الحكومية المتعلقة بالتنصت والمراقبة الإلكترونية، في عام 1976، أن نسبة 68% من قضايا التنصت التي تم التبليغ عنها تتعلق بمحاولات من قبل الزوج أو الزوجة للحصول على دليل لاستخدامه ضد الآخر في مسألة عائلية. ونسبة 11% كانت نتيجة نوع آخر من المراقبة المترلية تتضمن مراقبة من قبل الأهل أو بهدف التودد والغزل. هذا يعني أن نسبة 80% تقريباً من قضايا المراقبة والتنصت كانت تحدث ضمن العائلة. بالرغم من صدور هذا التقرير في الأيام ما قبل ظهور الحواسب وتركيزه على عمليات المراقبة من خلال خطوط الهاتف، فلا داعي للظن أن الإحصائيات قد تغيرت كثيراً على مر السنين، أما حالياً فقد تطورت وسائل التجسس حيث بإمكان الزوجة أو الزوج استعمال برنامجاً لمراقبة لوحة المفاتيح أو برنامجاً للتنصت لأهداف المراقبة.

بالنسبة للتنصت الذي يقع بين الزوجين، يوجد هناك قانون للسوابق يتعامل مع مثل هذه القضايا، وبالرغم من أن معظم هذه الحالات تتعامل مع تسجيل المكالمات الهاتفية بشكل سري، إلا أن العنوان iii يطبق أيضاً على التنصت الحاسبي. ومن ناحية أخرى لم ينتشر الكثير من القضايا المتعلقة ببرامج التنصت الحاسبية المختلفة، لكن نتائج القضايا السابقة المتعلقة بالتسجيل الهاتفي مرتبطة بالمحامين والقضاة.

عموماً، اتبعت المحاكم طريقين فيما يتعلق بانتهاكات العنوان iii من قبل أحد الزوجين:

- **استثناء "بيت الزوجية"**. في عام 1974، خلال قضية الزوجين Simpson (لا تتعلق هذه القضية بقضية اللاعب الأمريكي المشهور O.J.Simpson)، حيث قام الزوج بتسجيل مكالمات زوجته الهاتفية بشكل سري، أسست المحكمة الفدرالية استثناء للعنوان iii سمي بالاسم "بيت الزوجية"، وذلك انطلاقاً من أن نية هذا القرار هي عدم التدخل في الشؤون المترلية، وذلك بالرغم من عدم وجود هذا الاستثناء في القانون. وقد بنيت عدة قرارات لمحاكم أخرى على قضية الزوجين Simpson.
- **دون استثناء**. في عام 1976، خلال قضية السيد Jones ضد حكومة الولايات المتحدة، غيرت محكمة الاستئناف الفدرالية قرار المحكمة البدائية والتي أبعدت التهمة التي وجهها العنوان iii لزوج كان يعترض مكالمات زوجته غريبة الأطوار. صرحت المحكمة "إذا قصد الكونغرس إيجاد استثناء آخر للعنوان iii فيما يتعلق بالتنصت المرفوض على المكالمات الهاتفية، سيكون قد ضمن استثناءً معيناً للتنصت الزوجي في القانون." بالرغم من عدم انتشار الكثير من هذه المحاكمات في المحاكم الفدرالية فقد وافقت أغلبية القضايا الفدرالية وفي الولايات مع وجهة نظر السيد Jones.

وبالتالي إذا كنت تتنصت أو تراقب البريد الإلكتروني لزوجتك أو زوجك، بالرغم من أن هذا أمر غير ثابت، فإنك من المؤكد تتلاعب مع انتهاك للعنوان iii. لكن الشيء المؤكد هو أن المحاكم أوضحت بشدة أن أي فريق ثالث من طرف أحد الزوجين يقوم بالتنصت على الزوج الآخر في مترله بطلب من أحدهما فهو بالتأكيد ينتهك العنوان iii. (إذا كنت تقيم علاقة غير شرعية وقمت بالتنصت على الطرف الآخر فإنك في خطر بالتأكيد خاصة إذا كان طرفك الآخر مولعاً بالدعاوى القضائية).

ماذا عن مراقبة أطفالك؟ في هذه الحالة أيضاً يوجد قانون للسوابق، وهو مبني في معظمه على حالات متعلقة بالطلاق حيث يقوم أحد الأبوين بتسجيل المكالمات الهاتفية بين الطفل والأب الآخر. أوجدت الكثير من القضايا في المحاكم استثناء الأب-الطفل للعنوان iii مبني على القبول بالنيابة. عموماً، أقرّت المحاكم أن باستطاعة الوالد الذي يتولى رعاية الطفل أن يراقب اتصالات طفله القاصر طالما يعتقد الوالد أن هذه المراقبة هي من مصلحة الطفل. فإذا استخدمت برنامج مراقبة لوحة المفاتيح مثلاً فإنك لا تكون في خطر كبير إذا راقبت أطفالك بالمقارنة مع التهديد الذي تتعرض له إذا راقبت زوجك أو زوجتك، مع أن العنوان iii لا يمنح استثناء للوالدين. ومن جهة أخرى عندما يبلغ طفلك سن الرشد فلا يمكن تخمين النتيجة. (ملاحظة للأطفال الجواسيس: قد ينقذك سنك من السجن إذا كنت تتطفل على حاسب أبويك وتم الإمساك بك، لكن تذكر قد لا يكون الأبوان متساهلين مع معاقبة الأطفال كما تكون المحاكم في بعض الأحيان).

تلخيص

كما رأيت من خلال هذا الفصل توجد مجموعة من القوانين الفدرالية والحكومية المرتبطة بالتنصت الحاسي. ليس عليك أن تكون محامياً حتى تطّلع على هذه القوانين، أما التعامل مع تفاصيل هذه القوانين فهي مهمة المحامين.

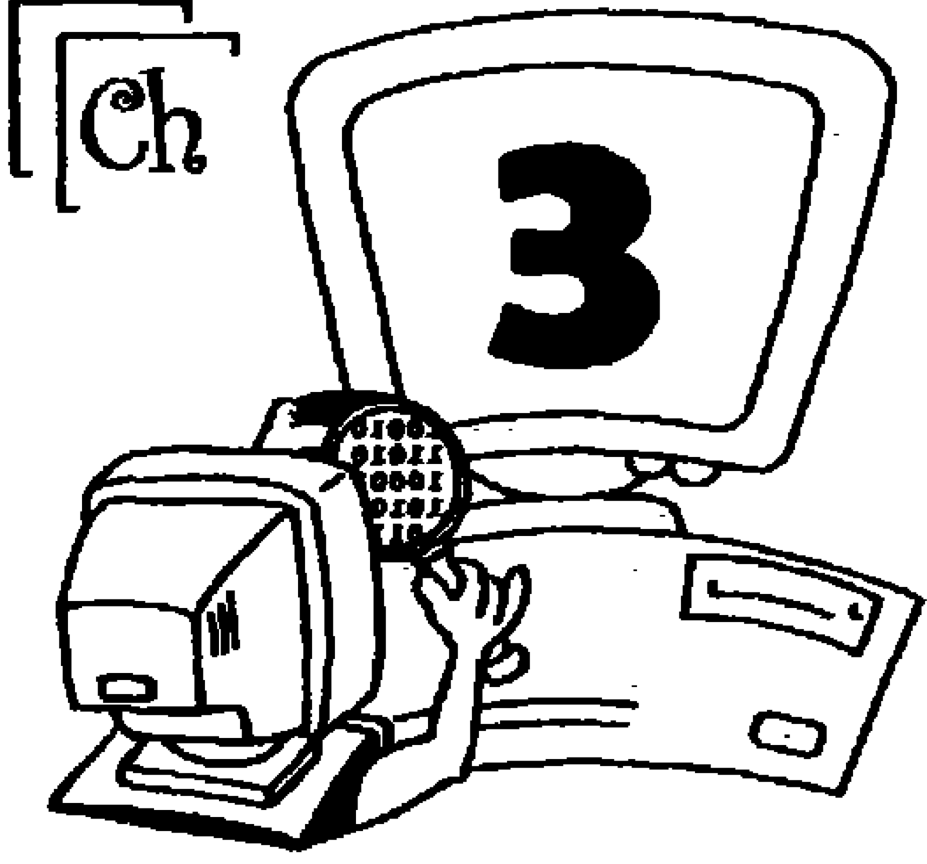
عليك ملاحظة ثلاث نقاط تتعلق بالتشريع الحاسي (سواء كان يتعلق بالتجسس أم لا):

- **لم يقم القانون بمجاراة التقنيات الحالية.** لقد تخلفت جميع القوانين التي تم تشريعها والقضايا التي تمت معالجتها عن تطورات تقنيات الشبكات، التجهيزات، والبرمجيات، حيث يمكننا تقدير التخلف الحاصل بعدة سنين فيما يتعلق بالشؤون القانونية والتقنية الحديثة. يحاول المحامون والمحاكم تعويض ما فاتهم، لكن التكيف مع التقنيات الحديثة سيشكل صعوبة كبيرة للنظام ككل.

- **القوانين ليست لمصلحتنا.** إن الفكرة السائدة بأنه تم تشريع القوانين لمصالح المجتمع هي فكرة ساذجة قليلاً (نحن نعلم ما هي مصلحتك لذلك عليك أن تضع كامل ثقتك بالقانون). تم إرسال المرسوم الوطني الأمريكي USAPA من خلال الكونغرس دون أي اعتبار للمشاعر الوطنية. يتضمن قرار أمن الوطن (Homeland Security Act)، الذي صدر في شهر كانون الأول عام 2002، تدابير تتعلق بالمراقبة دون الحاجة إلى أوامر مثول أمام المحكمة أو إشرافاً من قبل المحكمة. حدد اقتراح أولي لما تدعوه وزارة العدل بقرار تعزيز الأمن المنزلي (Domestic Security Enhancement Act) الملقب بالمرسوم الوطني ii، ظهر في شهر شباط من عام 2003 ويمنح الحكومة سلطات تجسس كبيرة. يجب أن يتوقع مستخدمو التقنيات قوانين غير منطقية أبداً.

- **القوانين تتغير.** التغيير لا فرار منه وهذا يطبق أيضاً على القانون. بالرغم من أن التغيير الشرعي لا يكون سريعاً جداً مثل تطور وتغير التقنيات، لكن قد لا تكون الأمور غداً كما كانت عليه البارحة. تجعل القوانين الجديدة، الآراء القانونية، والقضايا التي تمت معالجتها حسب القوانين القديمة المحامين مستعدين دائماً، كما يجب أن يكون الوضع نفسه مطبق عليك أو على منظمتك. وما قد يكون قانوناً للمراقبة الإلكترونية اليوم سوف يصبح شيئاً مختلفاً تماماً السنة المقبلة.

والآن، بعد هذه المقدمة العامة للشؤون القانونية دعونا ندخل في الجزء الأكثر تشويقاً من الكتاب (دون أي إهانة للمحامين): كيف نتجسس وكيف نمنع التجسس.



أعمال الحقيبة السوداء

نظرة إلى داخل الحقيبة السوداء

يمكن توضيح معنى المصطلح "أعمال الحقيبة السوداء" بأنه الاختراق والدخول الخفي لمبنى بهدف الحصول على معلومات أو دليل أو القيام بزرع نوع ما من أجهزة التنصت. لقد ظهر هذا المصطلح منذ فترة الحرب العالمية الثانية، عندما كان عملاء مكتب التحقيقات الفدرالي يحملون حقائب مثل حقائب الأطباء مصنوعة من الجلد الأسود لحمل المعدات من وإلى البيت أو المكتب المسروق. لكن المعنى الأصح لهذا المصطلح الخاص بقوى القانون من وجهة نظر سياسية لعمل الحقيبة السوداء (أو بشكله المختصر "عمل الحقيبة") هو "الدخول الخفي"، والذي لا يتمثل بهذا المعنى الإجرامي.

بالرغم من أن اختراق الأماكن التي ليس من المفروض أن تتواجد فيها وسرقة أسرار الآخرين هو عمل بدأ منذ آلاف السنين، إلا أن أول عمليات السطو المنظمة الحديثة لأهداف استخباراتية ظهرت في عام 1920، حين قامت البحرية الأمريكية بتمويل سلسلة من أعمال الحقيبة السوداء ضد الحكومة اليابانية. اقتحم العملاء الأمريكيون القنصلية اليابانية في مدينة نيويورك، بعد التعاون المشترك بين مكتب الاستخبارات البحرية، مكتب التحقيقات الفدرالي، وشرطة المدينة، وقاموا بفتح الخزنة وصوّروا كتاب التشفير البحري الياباني. لقد عاد هذا الاقتحام بفائدة عظيمة في سنوات ما قبل الحرب لأنه مكنّ الأمريكيين من قراءة الرسائل اليابانية التي تم اعتراضها وفك تشفيرها. واستمرت أعمال الحقيبة السوداء ضد اليابانيين حتى عام 1939، مع سلسلة من الاقتحامات الناجحة المنفذة ضد مكاتب حكومية يابانية أخرى واقعة في نيويورك.

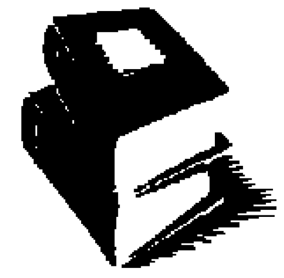
منذ الأيام الأولى لأعمال الحقيبة السوداء، جعلت التطورات في التكنولوجيا هذه الأعمال أكثر تعقيداً وكلفة. توجد مدارس حكومية ومدارس خاصة، في جميع أنحاء العالم، تعلّم مهارات

الدخول السرية متخصصة للجيش، قوى القانون، وموظفي المجتمع الاستخباراتي. هذه المهارات غالباً ما تشق طريقها إلى القطاع الخاص من خلال العملاء السابقين ذوي تجربة عملية سابقة.

تتخذ أعمال الحقيبة السوداء شرعيتها، عند منح المحكمة ترخيصاً للوكالة القانونية أن تنفذ عملية دخول خفية بحثاً عن دليل أو عندما يتولى عمل ما تحقيقاً على نفقته الخاصة دون معرفة الموظفين، أو يمكن أن تكون غير شرعية، عند وقوع دخول خفي دون إذن. (تذكر أن ارتكاب مثل هذا الأمر بشكل غير قانوني يجعلك موضع تهم كثيرة مثل الاختراق والدخول والسرقة، والتي لا تتهاون فيها الشرطة والمحاكم عادة).

تتناسب أعمال الحقيبة السوداء بشكل خاص مع التجسس الحاسبي لعدة أسباب:

- بسبب الكمية الضخمة من المعلومات التي يمكن تخزينها على القرص الصلب والسهولة والسرعة النسبية التي يمكن أن تنسخ فيها هذه المعلومات بشكل سري، كما تزود عمليات الدخول السرية كمية كبيرة من المعلومات بزمن قصير.
- من وجهة نظر تقنية، بما أنه شاع استخدام التشفير الصلب والذي من الصعب جداً أو حتى من المستحيل اختراقه، فقد أصبحت أعمال الحقيبة السوداء مثل التي استخدمت لمراقبة لوحة المفاتيح الخاصة بالمجرم Nicodermo Scarfo هي الطريقة الوحيدة المتبقية لقوى القانون. (قد تسبب المتطلبات القانونية المتساهلة لمثل هكذا عمليات تلصص بموجب تدابير المرسوم الوطني الأمريكي ازدياداً كبيراً لأعمال الحقيبة السوداء في السنوات القادمة).



لمزيد من التفاصيل عن قضية Nicodermo Scarfo الأصغر، انظر الفصل الثامن.

سوف تتعلم في هذا الفصل الأنواع المختلفة لأعمال الحقيبة السوداء، كيفية تنفيذها، وبعض الوسائل العامة لحمايتك منها.

أعمال الحقيبة السوداء الفيزيائية والشبكية

يمكن أن يقع عمل الحقيبة السوداء في أي مكان – منزل الضحية، مكتبه، سيارته، أو غرفة الفندق. فعلى سبيل المثال، حين قام مكتب التحقيقات الفدرالي بإجراء التحقيقات المتعلقة بموظف في وكالة الاستخبارات المركزية Harold Nicholson والمشتبه بتجسسه لصالح الروس، قام العملاء سرياً بتفتيش شاحنته الرياضية Chevrolet Lumina واكتشفوا حيازته على حاسب شخصي محمول، فقام العملاء بصنع صورة من قرصه الصلب، واكتشفوا لاحقاً وجود مستندات

سرية محذوفة خاصة بوكالة الاستخبارات المركزية، كما وُجد في الشاحنة أيضاً قرص مرن يتضمن معلومات حول عملاء الوصول، مواطنين أمريكيين يسافرون بصورة متكررة إلى الخارج ويزوّدون الوكالة بالمعلومات. لقد لعب هذا الدليل دوراً أساسياً في إدانة Nicholson.

أما عندما نتحدث عن التجسس الحاسبي، فيوجد لدينا نوعان عامان من أعمال الحقيبة السوداء:

- **المهاجمات الفيزيائية**. وهي عمليات سطو تقليدية، حيث يدخل الجاسوس مكاناً ما يفترض ألا يتواجد فيه. تخيل كسر الأقفال، أجهزة الإنذار، وأخيراً الممثل الشهير Tom Cruise وهو معلق بالمقلوب فوق حاسب. هناك مجازفة وخطر كبير أن يتم الإمساك بك خلال عملية فيزيائية وخاصة من قبل أناس يشكون بتصرفاتك. كما أن قوى القانون ماهرة جداً في التحقيق والاستجابة لعمليات السطو لأن عمليات السطو الإجرامية التي تستهدف أماكن السكن أو العمل شائعة جداً.
- **المهاجمات عبر الشبكات**. يستطيع الجاسوس، بدلاً من اختراق موقع فيزيائي، الاختراق عبر اتصال شبكي بهدف جمع المعلومات. إذا تم إنجاز عمل الحقيبة السوداء عبر الشبكة بصورة صحيحة فهي تشكل خطراً أقل بكثير من العمل الفيزيائي، لأنه أسهل بكثير أن تخفي آثارك في العالم الافتراضي مقارنة مع العالم الحقيقي. كما أن قوى القانون لا تمتلك التدريب والخبرة والموظفين الأكفاء للتعامل مع اختراقات الشبكة كما هو الحال مع الاختراقات الفيزيائية. إن من سلبيات المهاجمات عبر الشبكة أن المعلومات الموجودة على الحاسب هي الدليل الوحيد الذي يمكن الاستفادة منه، بالمقارنة مع المهاجمات الفيزيائية حيث يمكن إيجاد جميع أنواع المعلومات غير الرقمية المشوقة.



يركز هذا الفصل على المهاجمات الفيزيائية، لمعلومات أكثر عن التقنيات التي قد يستخدمها الجاسوس أثناء المهاجمات الشبكية، انظر الفصل العاشر.

مضبوط: البوابة المائية "السبّاكون"

لعل من أشهر الأمثلة عن أعمال الحقيبة السوداء المعروفة في التاريخ تلك التي حصلت في بناء المكاتب في واشنطن عند اللجنة الديمقراطية الوطنية. وقد أقر البيت الأبيض عملية السطو التي وقعت في السابع عشر من حزيران (يونيو) عام 1972، وكان البيت الأبيض وقتها متبنياً عمليات السطو غير الشرعية باستخدام وحدة تحقيقات خاصة تلقب بالاسم "السبّاكون Plumbers"، وهي مجموعة من عملاء استخبارات وقوى قانون سابقين معينين لتحديد وكشف أخطاء الحكومة لوسائل الإعلام.

- استخدم الرجال الخمسة الذين قاموا بتنفيذ العملية التي سميت "البوابة المائية Watergate"، معدات تجسس متطورة مستخدمة من قبل وكالة الاستخبارات المركزية، شملت كاميرات تصوير، أدوات لفتح الأقفال، آلات مصغرة للغاز المسيل للدموع، تجهيزات التنصت، وأجهزة الراديو. اقتحمت الوحدة بناء المكاتب خلال عطلة Memorial Day وقامت بزرع أجهزة التنصت، لكنها عادت مرة ثانية عندما لم يعمل أحد أجهزة التنصت. بالرغم من أن معظم أفراد وحدة السباكين هم من عملاء وكالة الاستخبارات المركزية ومكتب التحقيقات الفدرالي أو ممن لهم اتصالات بوكالة الاستخبارات المركزية، لكن هذه المهنة القذرة أدت إلى سقوطهم. حيث نسي أحد أفراد الوحدة إزالة شريط من ممسكة باب لجعله مفتوحاً، اكتشف أحد رجال الأمن هذا واتصل بالشرطة.

كتب أحد اللصوص، Eugenio R. Martinez مقالاً ممتازاً عن الاقتحام مع تفاصيل عن المهنة والفشل التقني. للحصول على المقال اتبع الرابط التالي:
www.watergate.info/index.php?itemid=18.

أعمال الحقيبة السوداء الانتهازية والمستهدفة

تأتي أعمال الحقيبة السوداء بنكهتين مختلفتين: مستهدفة وانتهازية. من أحد الأهداف الأساسية لعمل الحقيبة هو إنجاز العمل بشكل غير مكشوف، يجب ألا تعرف الضحية أنه تم اختراق أمنه أو أمنها

(أو ربما في وقت متأخر جداً). توجد طريقتان لتنفيذ عمل الحقيبة السوداء:

- **طريقة مستهدفة**. إن السمة المميزة لعمل جيد هو التخطيط الموسع. يمكن التفكير بالعملية بكاملها قبل وقوعها بوقت طويل. يكون التخطيط حرجاً بشكل خاص إذا كانت العملية معقدة بسبب أجهزة الإنذار، الحراس، الكلاب، أو إجراءات أمنية فيزيائية صارمة.

كلما زادت الإجراءات المضادة والحماية التي يملكها الهدف، كلما زادت الحاجة للتخطيط والموارد المطلوبة لتنفيذ هذا العمل. (بالطبع، يمكن أن تفشل أي عملية حتى مع الكثير من التخطيط والمنفذين ذوي الخبرة، خذ عملية البوابة المائية كمثال).

- **طريقة انتهازية**. ببساطة شديدة أعمال الحقيبة السوداء الانتهازية هي عملية سرقة المعلومات عندما تسنح الفرصة، يتجه الجاسوس إما ليحصل على أنواع محددة من المعلومات، أو يخمن أن مديره أو مديره الضمني قد يكون مهتماً لهذه المعلومات.

لا تحتاج هذه العمليات تقريباً إلى تخطيط، ولكن فرص نجاح العمليات الانتهازية تتناقص بشكل كبير عند وجود سياسات أمنية في المكان المستهدف، و يتم تطبيقها وتبنيها كعادة

من قبل الموظفين. سوف نوضح هذه الفكرة بتفصيل أكبر في فقرة "الإجراءات المضادة" من هذا الفصل.

وأخيراً، يتعلق إنجاز عمل الحقيبة السوداء بالأمور الاقتصادية. قد تجعل الظروف العملية مكلفة جداً من ناحية الزمن، المال، والخطر.

أساليب الجواسيس

في الكثير من فصول هذا الكتاب، لدينا فقرة مثل هذه تسمى "أساليب الجواسيس" والتي تصف كيفية كشف الجواسيس للمعلومات البالغة الدقة. غالباً ما نطلب منك أن تمثل دور الجاسوس لكي تفهم بشكل أفضل كيفية عمله أو عملها، أحياناً سوف تكون فتى جيد، وأحياناً أخرى لن تكون كذلك. إن التفكير بعقل الجاسوس هام جداً لتطوير طرق الحماية ضده.

ألعاب الجواسيس

لنبدأ بتمثيل دور الجاسوس، تخيل أنك تعمل مستشاراً لصالح شركة أمن متخصصة في اختبارات الاختراق وهي تقييم الأمن الفيزيائي أو الحاسبي لمنظمة أو كلاهما معاً. لقد استخدم الجيش والحكومة اختبارات الاختراق لعدة سنوات من أجل الوصول إلى أمن التسهيلات النووية، تركيبات الجيش، والشبكات السرية. تقوم "فرق النمر Tiger Teams" أو "الفرق الحمراء Red Teams" بشن مهاجمات ضد التسهيلات الأمنية أو الشبكات الحاسبية وذلك لاختبار ردود فعل التحديد والاستجابة. بعد الانتهاء من اختبارات الاختراق يتم إعداد التقارير التي توضح باختصار نقاط القوة والضعف الأمنية بهدف دعم طرق الحماية من المهاجمات والإجراءات المضادة. لقد شاع اختبار اختراق الشبكة الحاسبية للقطاع الخاص في السنوات الماضية وذلك لمحاولة الأعمال التجارية والحكومة عدم إدخال المخرّبين إلى شبكاتها.

هدفك الافتراضي هو قسم المبيعات لشركة برمجيات كبيرة، تقع الشركة في بناء مكاتب على بعد عدة أميال من حرم رؤساء الشركة المشترك. لقد قلق نائب رئيس قسم المبيعات أن المنافسون كانوا قد حصلوا بطريقة ما على مواد تدريب المبيعات حول المنتجات الجديدة التي لم تصدر بعد ويستخدمون المعلومات المناسبة لصالحهم. فقام باستخدام شركتك لتنجز تدقيقاً داخلياً كاملاً. بالرغم من تركيز فريق آخر على نقاط الضعف المحتملة في الشبكات، تكمن مهمتك في الوصول إلى الأمن الفيزيائي للمبنى ومحاولة اختراق المكتب.

بما أنك قد حصلت على الإذن لتكون جاسوساً، وقد حصلت على رسالة موقعة من نائب رئيس الشركة الأعلى بالإضافة إلى رقم جهاز الخلوي ورقم جهاز النداء الخاص به، هذا يعتبر ضماناً في حال تم القبض عليك، لكن لم يتم القبض على أحد من قبل من شركتك أثناء إنجاز العمل وأنت سوف تتابع بنفس الطريق.

بما انك جديد على كل هذا، قبل أن تفكر في كيفية تنفيذ مهمتك القادمة، فمن الجدير إلقاء نظرة على كيفية عمل جميع المحاسن والمساوئ، عليك التركيز فقد تحصل على بعض الأفكار.

في قلب عمل الحقيبة السوداء الحكومي

لا تتوفر الكثير من المعلومات بين العامة عن أعمال الحقيبة السوداء، وذلك لأن الأشخاص الذين ينفذون هذه الأعمال هم من (الجيش، قوى القانون، ووكالات الاستخبارات) ويحرصون على حماية مصادرهم وأساليبهم. حيث إذا تم كشف تقنيات أعمال الحقيبة، سيقدر الأشرار أن يأتوا بطرائق جديدة لمواجهتها. (من المؤكد أن هناك استحقاقات للمحافظة على الأمن العملي، لكن كما في جميع أشكال الأمن من خلال الغموض، يُترك المواطنون الملتزمون بالقانون والأعمال والذين قد يكونون ضحايا لأعمال الحقيبة السوداء غير الشرعية دون حماية تذكر لأنهم لا يعلمون ما هي الصعوبات التي تواجههم).

شارك العميل السابق لمكتب التحقيقات الفدرالي Wes Swearingen من سنة 1951 حتى 1977 ومؤلف الكتاب "أسرار FBI: عرض عميل FBI Secrets :An Agent's Expose"، في كثير من أعمال الحقيبة السوداء لصالح مكتب التحقيقات الفدرالي. زود من خلال كتابه ومن خلال مقابلات صحفية متعددة، تفاصيل عن "سوقيات أعمال الحقيبة السوداء". بالرغم من أن المعلومات مؤرخة وموجهة بصورة ما تجاه أعمال الحقيبة لمنازل المواطنين، فإن هذه المهنة التجارية ما تزال سارية حتى اليوم وتقدم إطاراً عاماً حول كيفية القيام بعمليات دخول سرية للمكاتب، المستودعات، وغيرها.

الفرق

يتمتع رجال مكتب التحقيقات الفدرالي وغيره من وكالات الاستخبارات بإمكانية استخدام عدة أشخاص خلال عمل الحقيبة السوداء، ويتحمل كل شخص مسؤوليات مختلفة، بينما يمكن لعميل منفرد أن ينفذ العملية، لكن استخدام مجموعة من العملاء للعملية لينجزوا مهام مختلفة أكثر أماناً. يمكن أن تتضمن عملية واحدة خمسة فرق وظيفية وهي:

- **التعقب.** يتتبع فريق التعقب سرياً الأشخاص الذين يقيمون أو يرتادون المكان بعد خروجهم من مكان السكن. تتلخص مهمة فريق التعقب في إعلام الفرق الأخرى عن مكان تواجد الأشخاص الذين يتبعونهم، لكي لا يعودوا إلى المكان المطلوب بغتة ويفاجئوا العملاء.
- **الداخلي.** الفريق الداخلي مسؤول عن دخول المبنى وتثبيت أجهزة المراقبة أو الحصول على دليل. يمكن تضمين خبراء المراقبة الإلكترونية، خبراء الحواسب، خبراء التصوير، و خبراء في حقول أخرى في هذا الفريق، بناء على الضرورة.
- **الالتقاط.** يقوم فريق الالتقاط بترك والتقاط الفريق الداخلي في منطقة مختارة لجذب أقل قدر ممكن من الانتباه إلى العملية.
- **المراقبة.** يراقب فريق محيط جوار المبنى من أي أشخاص أو أعمال التي قد تسبب في كشف العملية.
- **القيادة.** يوجّه فريق القيادة العملية من منطقة خارج المبنى، يمكن أحياناً لفريق القيادة أن ينجز مهام المراقبة أيضاً.

يتعلق عدد الأشخاص الذين يتم ضمهم لكل فريق بالهدف المطلوب وبالظروف المحيطة. مثلاً يستطيع شخص واحد أن يقوم بمهام القيادة والمراقبة في عملية بسيطة، بينما قد تتطلب عملية أكثر تعقيداً فرق تعقب متعددة لتراقب الهدف مشياً على الأقدام، في السيارات، وفي الجو.

أساليب: الفرق الداخلية السرية لمكتب التحقيقات الفدرالي

يصف مؤلف كتاب "فوق القانون Above the Law" David Burnham الذي ألفه عام 1996، باختصار برنامج الدخول السري الخاص بمكتب التحقيقات الفدرالي. يتضمن هذا البرنامج عملاء ذوي تدريب عالي المستوى، تكمن مهمتهم في الاقتحام السري لجميع الأماكن الممكنة من أجل جمع الأدلة وزرع أجهزة المراقبة. يوجد اختصاران مرتبطان بعمليات المراقبة لمكتب التحقيقات الفدرالي: الأول SOG والذي يشير إلى Special Operation Groups أي مجموعات العمليات الخاصة والتي تكون مسؤولة عن المراقبة الفيزيائية والإلكترونية، والاختصار TTA الذي يشير إلى Technically Trained Agents أي العملاء المدربون تقنياً، والذين يتمتعون بمهارات المراقبة الإلكترونية أو المهارات الحاسبية الضرورية لتنفيذ هذه العمليات السرية.

بالرغم من رفض مكتب التحقيقات الفدرالي مناقشة برنامج الدخول السري، إلا أننا نعلم جيداً من شهادات خطية متعددة مع قَسَم المنتشرة علناً أن البرنامج فعال جداً. أنجز مكتب التحقيقات الفدرالي أعمال الحقيبة السوداء في عدة قضايا بارزة في المنازل، المكاتب،

والسيارات من أجل جمع الأدلة ضد المشتبه بهم، من هذه القضايا قضية Aldrich Ames، Robert Hanssen، Ana Belen Montes، وBrian Regan، بالإضافة إلى القضايا الجنائية مثل قضية Nicodermo Scarfo.

يتم تنفيذ عمليات الحقيبة سواء لصالح مكتب التحقيقات الفدرالي أو وكالات فدرالية أخرى، بموجب قرار من المحكمة، عموماً يجب المرور بأربع مراحل:

- يصرّح مكتب التحقيقات الفدرالي أو وكالة فدرالية أخرى ترغب بتنفيذ المراقبة الإلكترونية عن طلباتها.
- يفحص العملاء التقنيون سرياً الهدف ويجمعون المخططات الهندسية التفصيلية.
- يجمع الفريق كافة الأدوات التي يحتاجها لأداء المهمة، بما فيها معدات المراقبة المصممة خصيصاً للمهمة.
- يقوم الفريق بعملية الدخول.

سوف يشهد برنامج الدخول السري عملاً أكثر في أعقاب الهجمات المثيرة للجدل في 11/9. طلب مكتب التحقيقات الفدرالي بالنسبة لميزانيته المالية السنوية عام 2003 زيادة بقيمة 12,162,000 دولار أمريكي من أجل أمر سموه "العمليات التكتيكية"، وُصف هذا العنصر "... لتحسين قدرة مكتب التحقيقات الفدرالي على الاستجابة لطلبات التفتيش الفيزيائية المتزايدة ولتوجيه التطورات في التقنية عبر البحوث، التطوير، والهندسة."

كما أن المكتب مهتم بتعزيز برنامج العملاء المدربين تقنياً TTA، كما اقتبس من نص طلب زيادة الميزانية المالية لعام 2003، "يشكل الاستخدام المنتشر لتقنيات الاتصالات الرقمية واندماج ميزات وقدرات السرية من خلال استخدام التشفير، تحدياً خطيراً للمكتب. يستخدم المجرمون هذه التقنية لتغطية عملياتهم السرية ولمقاومة جهود قوى القانون. يتضمن طلب الميزانية المالية لعام 2003 بالقيمة 10,027,000 دولار أمريكي تمويل الموظفين لعملاء TTA جدد وذلك لدعم إدارة المكتب بجميع وظائف المراقبة وتزويد معدات ضرورية لعملاء TTA الحاليين بالإضافة إلى دعم تدريب المتطوعين لضمان امتلاك عملاء TTA جميع الخبرات التقنية لتنفيذ عمليات المراقبة الإلكترونية والاستجابة السريعة والفعالة للتقنيات الصاعدة."

مع صدور المرسوم الوطني الأمريكي، أعرب الكثير من جماعات الحريات المدنية عن قلقهم حول القيود المخففة للمراقبة والمفاسد المحتملة بناء على تاريخ أمريكا. حيث قام مكتب التحقيقات الفدرالي منذ الحرب العالمية الثانية حتى منتصف السبعينيات بمئات أو حتى آلاف أعمال الحقيبة السوداء غير الشرعية على رجال السياسة، الناشطين ومنظمات الحقوق المدنية، وحتى المواطنين العاديين. لا أحد يعرف ربما التاريخ يعيد نفسه.

الأبحاث والتخطيط

لا يهرع العملاء بعد حصولهم على موافقة من القاضي لتنفيذ عملية الحقيبة السوداء، حيث يجب إنجاز كمية لا بأس بها من البحوث والتخطيط قبل التنفيذ. توجد علاقة سلبية بين الخطر والتخطيط، فكلما زاد التخطيط نقص الخطر، وبالعكس. بالرغم من أنك لا تستطيع أن تقضي على الخطر بشكل كامل، إلا أن التخطيط والبحوث يخففان الخطر ويزيدان من فرص النجاح.

فيما يلي بعض المعلومات الأساسية الواجب تحديدها خلال طور البحث والتخطيط:

- **الهدف**. ضد من ستنفذ هذه العملية. تنشأ صورة الضحية من السجلات والمراقبة متضمنة قنوات القيادة، الاجتماعات والأحداث التي يتم حضورها بشكل دوري، والهوايات والأساليب التي تسّهل تعقب الهدف.
- **رمز الهدف ومكان عمله**. تقع معظم أعمال الحقيبة السوداء عندما يكون الهدف في العمل، لذلك من الهام جداً معرفة وقت ومكان عمل الهدف بالإضافة إلى نوع العمل.
- **الأشخاص الذين يقيمون مع الهدف (أو الذين يزورون الهدف)**. قبل أن يقدم العملاء على تنفيذ العملية، يجب معرفة فيما إذا كان المبنى خالياً، كما يجب معرفة عدد الأشخاص المقيمين مع الهدف، مع خطط جاهزة لكل شخص منهم.
- **ملكية العقار (إذا لم يكن ملك الهدف)**. قد يسعى الأشخاص العاديون للتعاون مع مكتب التحقيقات حتى دون وجود رخصة، قد يقدم مالك العقار الكتوم خدماته ويدع العملاء للدخول بكل بساطة.
- **معلومات عن مكان الإقامة**. تتضمن هذه المعلومات صوراً، ملاحظات مكتوبة عن الأبواب، الأقفال، الإضاءة، المخططات الهندسية، الحيوانات الأليفة، الجيران، وتفاصيل أخرى قد تكون مفيدة عند التخطيط للعملية. يجب جمع هذه المعلومات بصورة خفية لكي لا يلاحظ الهدف أنه تحت المراقبة.

اعتماداً على هذا البحث يتم تطوير خطة لتحقيق غاية معينة، مثل زرع جهاز تنصت أو الحصول على دليل ممكن من الحاسب. يتم الاحتفاظ دائماً بخطة للطوارئ في حال لم تنفذ العملية كما تم خُطط لها، وتحدد الأدوات المتخصصة والمعدات اللازمة للعملية، عدد العملاء المطلوب بما فيهم العملاء ذوي المهارات الخاصة، كما يتم إطلاع العملاء في كل فريق باختصار على الخطة.

عملية الاختبار

التدريب يصنع الكمال، ويتمنى مكتب التحقيقات الفدرالي أن تسير العملية كما خطط لها تماماً دون أن تكشف، لذلك الخطوة التالية هي القيام بعملية اختبار قبل بدء العملية. يكون تتابع الأحداث في عملية الاختبار كما يلي:

- يتبع فريق التعقب الهدف وأي أفراد آخرين يقيمون في نفس المترل عند خروجهم منه. يجب استخدام عميلين على الأقل لتعقب كل فرد بناءً على الظروف، وذلك بهدف تأمين مساندة واستمرار التعقب في حال تم كشف أحد العملاء عند مراقبته للفرد.
- يجب أن يبقى جميع أعضاء فريق التعقب على اتصال دائم بالراديو، إذا انقطع اتصال الراديو تتوقف العملية بكاملها. (لتجنب التنصت من قبل الناس ذوي الأدوات فاحصة، تستخدم جميع اتصالات الراديو رموز محددة سلفاً عند عدم توفر أجهزة راديو مشفرة).
- بعد خروج الهدف وجميع المقيمين في المترل مع ملاحقتهم من قبل فريق التعقب، يمكن البدء بالتجربة قبل التنفيذ الحقيقي.
- يجري العملاء اتصالات هاتفية مزيفة للجيران، الذين قد يشاهدوا عملية الدخول وبهدف صرف انتباههم عن العملية. يحدد العميل "الرجل الخارجي" في فريق القيادة والذي تتحدد مهمته بمراقبة وتوجيه العملية، الوقت الدقيق لإجراء هذه المكالمات.
- يوجه "الرجل الخارجي" "فريق الدخول" إلى الموقع المطلوب ويعلم فرق المراقبة عن بدء العملية. خلال عملية الاختبار يتم استخدام فريق مكون من شخصين، أحدهم لتزع أقفال الأبواب واختراق أجهزة الإنذار والآخر يتصل مع "الرجل الخارجي" عبر الراديو. (يمكن إضافة خبير تقني للفريق بناءً على الظروف).
- يقود فريق الالتقاط، والذي يمكن أن يتألف من عميل واحد، "الفريق الداخلي" إلى موقع محدد مسبقاً حيث لن تتم مشاهدتهم أثناء خروجهم من المركبة، ومن ثم يغادر فريق الالتقاط المنطقة مباشرة.
- يقترب فريق الدخول من المدخل الرئيسي ويبحث عن أنظمة الإنذار الواضحة، في حال لم تتواجد أي أجهزة إنذار يدخل الفريق المبنى، إذا تم اكتشاف أجهزة إنذار لا يمكن اختراقها يتم تدوين ملاحظات عنها من أجل محاولة قادمة. يُعلم عميل الاتصال "الرجل الخارجي" بأن الفريق أصبح في الداخل. (تستخدم الفرق تعابير لعبة البيسبول كرموز، مثلاً "أصبح اللاعبون في الملعب" للإشارة أن "فريق الدخول" أصبح في موقعه، بالطبع يمكن أن تختلف الرموز بين الفرق).

- تبدأ عملية الاختبار بتفتيش كامل بحثاً عن أي أشخاص قد يتواجدون في المكان، يشرح "فريق الدخول" جميع الأحداث "للرجل الخارجي" عند استيلاءهم على المبنى. يمكن أن يتم استدعاء المصور لالتقاط صور للدليل أو لتوثيق الأشياء الموجودة في الداخل من أجل الأعمال القادمة (خاصة الأعمال التي تتضمن زرع أجهزة تنصت، مثلاً يجب أن يكون جهاز التنصت مصمم خصيصاً ليتناسب مع قطعة أثاث أو أي شيء آخر في المترل). اعتماداً على كمية الوقت التي يستغرقها فريق الدخول لإتمام مهامه يتصل فريق التعقب للإعلام عن أهدافهم في حال كانوا سوف يرجعون إلى المبنى أم لا.
- يعطي "فريق الدخول" تقريراً بالتقدم "للرجل الخارجي" كل عدة دقائق، وعند الانتهاء يطلب الفريق أن يتم إخراجهم.
- بعد خروج "فريق الدخول" من المبنى، يتصل "الرجل الخارجي" بالعملاء المسؤولين عن التعقب والمراقبة ويطلب منهم التوقف عن المراقبة والعودة إلى المكتب.

العمل

بعد الانتهاء من تجربة الاختبار، يتم استجواب جميع الفرق، ما هي أجزاء المخطط التي نجحت، ثم يتم تنفيذ العملية الفعلية. تتبع العملية الشكل العام لعملية الاختبار، مع إمكانية إضافة خبراء تقنيين إلى "فريق الدخول".

تحتاج العملية الناجحة، والتي يصعب كشفها إلى الخبرة، التجربة، ومستوى عالٍ جداً من التنظيم. لا يتمتع الجميع بالموارد والمهارات لتحقيق النجاح في أمر كهذا، حتى مكتب التحقيقات الفدرالي يملك عدداً محدوداً من العملاء فقط لهذا النوع من العمل. تُستخدم أعمال الحقيبة السوداء في القضايا التي لم تنفع فيها التقنيات الأخرى لجمع الدليل وذلك بسبب الالتزام بالوقت والكلفة الكبيرة لهذه العمليات.

استغلال نقاط الضعف

والآن بعد أن حصلت على فكرة عامة حول كيفية عمل المحترفون، دعنا نعود إلى سيناريو كيفية التخطيط والتنفيذ لعمل الحقيبة السوداء ضد زبون لشركة البرمجيات الخاصة بك. لن ندخل بالتفاصيل، مثل كيف نخترق حساسات الإنذار أو نفتح قفل عالي الأمن Medeco (توجد مراجع في هذا القسم والتي تطلعك على معلومات حول هذا)، بدلاً من ذلك سوف نركز اهتمامنا على استغلال نقاط الضعف العامة والشائعة.

يمكن تشبيه أعمال الحقيبة السوداء نوعاً ما باختراق نظام الأمن الحاسبي: تبحث عن نقطة ضعف وتفكر في طريقة لاستغلالها، إلا أن أعمال الحقيبة السوداء معقدة أكثر لأنها تتضمن عوامل أمن كثيرة ولا يمكن تحديدها أو استغلالها بسهولة باستخدام أدوات برمجية.

البحث والتخطيط للعملية

اقتباس من مقولة قديمة،"التخطيط المناسب المسبق يمنع الأداء السيئ،" وبالإضافة إلى هذه المقولة هناك عناصر هامة عند التخطيط للعمل وهي:

- **الهدف**. ضد من ستنفذ هذه العملية. عليك دائماً تحديد أهداف وغايات العمل وتجميع أكبر قدر ممكن من المعلومات، يمكن أن تتضمن هذه المعلومات الهوايات الشخصية، وجود أجهزة إنذار أم لا، نوع أقفال الأبواب، أو نوع الحاسب الذي يستعمله الهدف.
- **الزمن**. سوف تتوفر لديك كمية محددة من الوقت لتتمكن من تنفيذ العملية، لذا من الهام جداً تحديد الفترة الزمنية التي يحتاجها كل جزء من العملية، قد لا يكون الزمن هو كل شيء لكنه بالتأكيد عامل هام.
- **التخاطب**. يشير التخاطب إلى الاتصالات، أي استخدام أجهزة الراديو بصورة خفية خلال تنفيذ العملية وضمان معرفة أعضاء الفريق بشكل واضح بمهامهم ومسؤولياتهم.
- **الأدوات**. تأكد من حيازتك على الأدوات المناسبة للعمل. بالنسبة للتجسس الحاسبي قد تتضمن هذه الأدوات الخدمات البرمجية التي تخترق نظام التشغيل وبرامج الأمن، تفحص الملفات، أو نسخ الأقراص الصلبة (لا تنس الأداة التي ستنسخ القرص الصلب إليها). قد تحتاج أيضاً إلى تجهيزات أو برامج لمراقبة ضربات المفاتيح في الحاسب أو للدخول إلى الشبكات.
- **الاستراتيجيات**. يجب تطوير خطة محكمة مع خطة للطوارئ في حالة وقوع أحداث غير متوقعة.
- **الحكاية**. يجب أن يكون لديك حكاية جاهزة مقبولة ومحبوكة جيداً في حال تم كشفك.

حان الوقت لتطبيق هذه المعلومات وإيجاد خطة لعمل الحقيبة السوداء للسيناريو، لديك شخصان لمساعدتك أثناء اختبار الاختراق، فيما يلي المعلومات الأولية التي جمعتها عن الهدف:

- مبنى المكاتب له مدخلان، الردهة الرئيسة في الطابق الأول وسرداب لوقوف السيارات، ولكل منهما أقفالاً ذات بطاقات حيث تحتاج لبطاقة تعريف تمررها عبر القارئ ليتم فتح

الباب. تحمي قارئات البطاقات المصاعد في ساعات عدم العمل ويتم تشفيرها إلى البطاقة، مثلاً إذا كان مكتبك في الطابق الرابع سيأخذك المصعد إلى هذا الطابق فقط. تملك السلالم أبواباً مزودة بأجهزة الإنذار، والتي تكون مقفلة دائماً من الخارج، وتُفتح عندما يتم تشغيل إنذار الحريق.

- خلال ساعات الدوام، أيام الأسبوع من الساعة 7:30 a.m. حتى الساعة 6:00 p.m.، توضع طاولة لخدمة الزبائن في الردهة الرئيسة. إن لم تكن موظفاً، ستقوم موظفة الاستقبال بإرسالك إلى الباب المقفول (تحت سيطرة قارئ البطاقة) أو تنادي أحداً من المكاتب ليرافقك ليحدد لك موعداً.
- خلال ساعات عدم العمل، يجلس حارس الأمن في مكتب الردهة. توجد ثلاث كاميرات مراقبة عند المكتب متصلة باثنتين في السرداب الخلفي وتظهر الجوانب المقابلة لموقف السيارات وأخرى تظهر مدخل المبنى الثاني من جهة السرداب. يوجد حارس واحد فقط يقوم بجولات مراقبة حول المبنى كل ساعة، عندما لا يقوم بجولاته يجلس على مكتب الردهة يطالع، يشاهد التلفاز، أو يلعب بألعاب الحاسب.
- تتم خدمة الحراسة كل يوم من أيام العمل مساءً حوالي الساعة 10:00 p.m. مع فريق صيانة مأجور.
- يحتل قسم المبيعات الطابق الرابع بكامله، تتضمن مكاتب جميع الموظفين أبواب مقفلة بدلاً من المقصورات. الموظفون في هذا القسم أكبر سناً، لديهم عائلات، ولا يأخذون ساعات عمل إضافية كما يفعل باقي الموظفين في الشركة.

ابدأ بالتفكير ما هي المعلومات الأخرى المطلوبة والتي قد تحتاجها لاختراق جهاز أمن المبنى الفيزيائي.

تحقيق الدخول

من الواضح أنك تحتاج إلى حاسب قبل أن يكون بمقدورك البحث عن معلومات أو دليل، قد يكون هذا البحث سهلاً جداً أو بغاية الصعوبة لأنه يجب أن تتجاوز عدة مراحل من أجهزة الأمن الفيزيائية للوصول أخيراً إلى البيانات المطلوبة. مثلاً في مبنى مكاتب، عليك تجاوز الردهة، المصعد أو السلالم، باب الجناح المقفل، ومن ثم باب المكتب.

عموماً توجد ثلاث طرق لتحقيق الوصول السري إلى الموقع المطلوب. بالترتيب الأقل خطورة إلى الأكثر خطورة تتضمن ما يلي، استخدام المطلعين، "الاستنباط" (الهندسة الاجتماعية)، والاقتحام ثم الدخول.

استخدام المطلعين

المطلع هو شخص يعمل، يعيش، أو لديه سبب ما ليكون في الموقع الذي تحاول الوصول إليه، عندما يتعلق الأمر بتحقيق الوصول إلى المعلومات البالغة الدقة يُفضل استخدام المطلعين دوماً للأسباب التالية:

- لديهم وصول مسبق للمعلومات
- المطلعون معروفون للأشخاص الآخرين في الموقع
- خطرهم أقل بكثير مقارنة مع إرسال شخص خارجي

عندما تقوم وكالات الاستخبارات الحكومية باستخدام أشخاص ليقوموا بالتجسس ضد وطنهم ولصالح أمريكا، فهم يبحثون عن مواصفات محددة فيهم وهي المال، طريقة التفكير، التسوية، والغرور- هذه من المحفزات الفردية أو الجماعية لتحويل شخص ما إلى جاسوس. تتضمن أنواع المطلعين المستهدفين ما يلي:

- **الموظفون المستاءون.** الموظفون الذين لم ينالوا ترفيعاً ويعانون من أعمال الانضباط ولديهم تأخير في الدفع أو الفوائد.
- **الموظفون الحساسون.** من لديه مديونية، إدمان على الكحول أو المخدرات، علاقات غرامية، أمور تتعلق بالصحة العقلية، أو مشاكل في العلاقات العامة.
- **المتعاقدون.** مثل عمال التنظيفات، حراس الأمن، عمال الإصلاح الذين لا يكونون مخلصين لعملهم مثل كإخلاص الموظفين ذوي الدوام الكامل.

بالرغم من أن توظيف الجواسيس وفقاً للمعايير الأربعة السابقة هو استراتيجية تجسس تدعمها الحكومة، إلا أنها تعمل بصورة جيدة أيضاً فيما يخص التجسس الاقتصادي.



الخيانة 101 هي موقع ويب ممتاز مخدّم من قبل خدمة الدفاع عن الأمن التابعة للجيش. يزود الموقع خلاصة عن الأسباب التي تجعل الناس يقومون بالتجسس، مناقشة مواضيع تجسس معاصرة، أمثلة التهديدات التي يشكلها المطلعون، معلومات حول كيفية القبض على الجواسيس، ومعلومات ديموغرافية وإحصائية عن الجواسيس. اتبع الرابط:

www.dss.mil/training/csg/security/treason/intro.htm.

مضبوط: عقل الجاسوس

يُعتبر Robert Hanssen أحد الجواسيس المدمرين في تاريخ أمريكا، حتى تم القبض عليه عام 2001، حيث قام Hanssen العميل العالي المستوى لصالح مكتب التحقيقات الفدرالي، ببيع أسرار الشعب إلى روسيا لمدة عشرين سنة، وحصل بالمقابل على أكثر من 1.4 مليون دولار أمريكي نقداً وبالماس.

Hanssen هو الجاسوس الأول الذي تم فضحه بصورة علنية. استخدم Hanssen الإنترنت استخداماً واسعاً وقد كان مستخدماً لنظام التشغيل Linux وماهراً تقنياً، اعتاد أن يرسل أسئلة إلى المجموعة الإخبارية USENET عن مشاكل التجهيزات، وحدات GPS (نظام تحديد الموقع الشامل Global Positioning System وهو نظام لتحديد الموقع تم تطويره من قبل وزارة الدفاع الأمريكية، حيث يمكن للمستخدمين عن طريق تجهيزات GPS عالية الكلفة تحديد موقعهم الجغرافي بدقة 100 متر تقريباً. يعتمد هذا النظام على 24 قمر صناعي تدور حول الأرض بمواقع ثابتة، حيث يمكن لأي مستقبل GPS على الأرض أن يلتقط الإشارة من أربعة أقمار على الأقل، ومن ثم الاستفادة من هذه الإشارة لتحديد الموقع)، أجهزة المساعد الرقمي الشخصي PDA، والكاميرات الرقمية (بالإضافة إلى بعض القصص المشوقة عن زوجته). لم يكن Hanssen مغفلاً فيما يتعلق بالتقنيات المعلوماتية ويمكن أن يتساءل أحدنا فيما إذا كان Hanssen يمرّر رسائل إلى الروس من خلال رسائل USENET التي تظهر باستمرار، مستخدماً اسمه الشخصي أو اسم مستعار.

مازال بريد Hanssen موجوداً في المجموعة الإخبارية USENET، في حال كنت مهتماً لإلقاء نظرة سريعة على عقل الجاسوس اتبع الرابط http://groups.google.com، وابحث عن عناوين البريد الإلكتروني التي استخدمها Hanssen، ومنها hanssen@orion.clark.net، hanssen@nova.org، hanssen@amelia.nas.nasa.gov، rphanssen@earthlink.net، أو TBERRR1@aol.com.

"الاستنباط" - الهندسة الاجتماعية

معروف باسم " الهندسة الاجتماعية " في مجال أمن الحاسب ومجتمعات القرصنة، ومعروف باسم "الاستنباط" في مجال التجارة الجاسوسية ويعني استخلاص المعلومات بلطف أو جعل أحد ما يقوم بشيء ما لمصلحتك خلال محادثة عادية جداً.

باعتبارها تقنية تجسس، يستغل الاستنباط عدة جوانب أساسية للطبيعة البشرية:

- يسعى معظم الناس أن يكونوا لطفاء ونافعين، فيقومون بالإجابة عن الأسئلة، حتى من الغرباء.
- يسعى معظم الناس أن يظهروا بأنهم مثقفون ومطلعون جداً، ويتكلمون أحياناً أكثر مما ينبغي.

- يرغب الناس أن يتم تقديرهم ويحسون بأنهم يقومون بعمل مفيد، وفي النتيجة يتحدثون من أجل مدح عملهم.
- يتردد الناس في إخفاء بعض المعلومات، الكذب، أو الارتياب بنوايا الآخرين.

تبدو عملية "الاستنباط" كجزء من محادثة عادية اجتماعية أو مهنية، عندما يقوم بها مختص ماهر ويمكن أن تحدث في أي مكان – مكان العمل، مناسبة اجتماعية، مطعم، مؤتمر، أو خلال زيارة لمنزل أحد ما. يمكن أن تكون بعض أنواع "الاستنباط" قانونية، مثل تجميع جاسوس لقطع من المعلومات من أشخاص مختلفين للحصول في النهاية على أداة لكشف معلومات سرية.

يمكن أن يتم "الاستنباط" عبر الهاتف (الأكثر أماناً) أو شخصياً، مثلاً، التظاهر بأنك عامل تصليحات، عامل توصيل، ممثل لشركة خدمية، موظف، أو أي شخص آخر يقرّبك إلى هدفك (تأكد أنك تتمتع بالمظهر المناسب ووثائق مزيفة لتنجح في عملك). يتم استخدام "الاستنباط" الشخصي وعبر الهاتف كجزء من خطة متكاملة لكشف المعلومات.

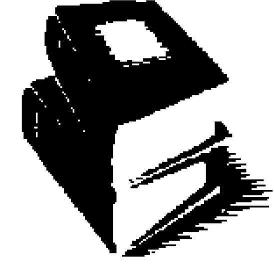
الاقتحام ثم الدخول

إن الطريقة الأخيرة والأكثر خطورة لتحقيق الدخول هي عن طريق الاقتحام ثم الدخول (B&E "Breaking AND Entering" بلهجة رجال الشرطة). تتضمن هذه الطريقة انتزاع الأقفال، سرقة المفاتيح، تجاوز أجهزة الإنذار، واستخدام أساليب سطو أخرى. يتجلى الاختلاف الأساسي بين الاقتحام الإجرامي العادي وعمل الحقيبة السوداء الجاسوسي في أن اللص يهتم عادة بسرقة شيء ما ذو قيمة مادية دون أن يهتم إذا ترك دليل وراءه، بينما لا يترك الجاسوس أي أثر لكي لا يعلم الهدف أنه كان ضحية عمل الحقيبة السوداء. (في بعض الحالات، يتم إنجاز عمل الحقيبة السوداء لكي تبدو مثل عملية سرقة لإبعاد الشكوك عن هدفها الحقيقي).

أصبحت علامات البطاقات، أزرار الأقفال، أجهزة الإنذار، الحراس، أجهزة التنبيه بقياس الحيوية التي وُجدت في المنشآت العالية الأمن، شائعة حالياً. تشكل إجراءات الحماية هذه تحدياً جدياً للجاسوس، في الحقيقة طالب مكتب التحقيقات الفدرالي، أثناء عدة مؤتمرات لتحديد الميزانية، بتمويل إضافي للبحوث والتطورات الحديثة، مصرحاً بأنه أصبح من الصعب جداً إنجاز عمليات دخول سرية على المنازل والمباني بسبب تطور تقنيات الأمن.

فيما يتعلق بعملية الاقتحام ثم الدخول، لا تشكل النوافذ والأبواب المداخل الوحيدة لحمايتها، قد يخترق فريق دخول خفي، أثناء تنفيذ عمل معقد وخاصة الموجه ضد هدف صعب، خلال الجدران، الأسقف، وحتى من الأرضيات لتحقيق الوصول. يمكن أن تستخدم الفرق العالية

المستوى أشخاصاً مختصين ليقوموا بإعادة كل شيء كما كان وتصليح نقطة الدخول بحيث لا تبدو أنه تم اختراقها.



إذا كنت مهتماً بطريقة عمل الأقفال وكيفية تجاوزها، فإن نقطة انطلاق الممتازة هي استخدام الأسئلة الشائعة للنشرة USENET على الرابط:
www.indra.com/archives/alt-locksmithing/.

تتضمن مجموعة الأسئلة عدداً من الموارد، بما فيها روابط لطرق انتزاع الأقفال.

للحصول على معلومات أكثر، اقتن كتاب Mark Tobias تحت عنوان الأقفال، الخزنات، والأمن والمتوفر بشكل إلكتروني على اسطوانة مضغوطة أو مطبوعاً. يشكل هذا الكتاب، المؤلف من 1,400 صفحة والمصور، مرجعاً نهائياً عن الأقفال والخزنات وكيفية تجاوزهم. الكتاب ليس رخيصاً لكنه للمحترفين. لمعلومات إضافية قم بزيارة الموقع www.securuty.org.

عودة الآن إلى السيناريو، ما هي الطريقة التي يجب عليك استخدامها للدخول إلى المبنى؟ هناك الكثير من الخيارات، لنأخذ أحدها والمؤلفة مما يلي:

عُرض للموظفين في الشركة الهدف عضوية في نادي الصحة التابع للشركة، كجزء من الفوائد المشتركة للموظفين. عبر قيامك بالمراقبة المستمرة تكتشف أن مدير قسم المبيعات يقصد النادي يومياً بعد العمل. (ظهر اسمه وصورته في مقالة لمجلة وجدتها على الموقع Google عند قيامك بالبحث في قسم المبيعات، ويملك موقعاً خاصاً باسمه للسيارة، لذلك فمن السهل الآن على أحد زملائك أن يتبعه ويكتشف هواياته). خطوتك الآن الاشتراك بعضوية مؤقتة في النادي والبدء بحديث مع مدير قسم المبيعات – طبعاً دون أن تكشف عن هويتك ونواياك الحقيقية. يمارس المدير رياضة كرة المضرب لذلك سوف تجلب معك في المرة القادمة مضرباً وتلعب عدة جولات معه. ثم يخبرك المدير عن رحلة التزلج التي سيقوم بها في أيام العطلة الثلاثة المقبلة.

الأمر الذي لا يدركه هو أنك تخطط لسرقة بطاقة الدخول الخاصة به من خزانة النادي قبل يوم رحلته بينما يستحم، وبما أنه مشغول برحلته فلن يلاحظ اختفاء البطاقة وفي حال لاحظ ذلك لن يعير هذا أي اهتمام حتى يذهب إلى عمله يوم الثلاثاء.

لقد قمت بنجاح بسرقة بطاقة الدخول، و في صباح يوم السبت تتوقف بك سيارة الأجرة على بعد شارع من الشركة وتتقدم باتجاه مدخل سرداب السيارات. تصطحبك امرأة، ويوجد داخل جيبك بطاقة الدخول المسروقة مع نسخة مطابقة لبطاقة هوية المدير لكن مع صورتك الشخصية عليها، وتبدو مشابهة تماماً لبطاقة الهوية الخاصة بالشركة، ثم تقوم بخفض رأسك أثناء تمرير بطاقة

الدخول في القارئ لكي لا تصورك كاميرا المراقبة، ينفتح الباب وتستخدم بطاقة الدخول نفسها للوصول إلى المصعد، بعد أن تدخل إلى المبنى تضع بطاقة الدخول في جيبك وتلصق بطاقة الهوية على جيب سترتك الأمامي، تملك مع شريكتك أجهزة راديو مع سماعات أذن بالكاد يمكن رؤيتها بحيث تبقى على اتصال مع زميلك الذي يراقب خارج المبنى فيما إذا دخل أحدهم فجأة، حيث يراقب الردهة الأمامية وعلى مرآه الحارس الجالس على المكتب ويقرأ الجريدة.

توثيق المشهد

بعد أن قمت بالدخول إلى الموقع المطلوب بنجاح، من الهام حالياً توثيق المشهد وهذا يعني ببساطة الاحتفاظ بسجلات عما واجهته وهذا متعلق بأعمال الحقيبة السوداء (من البديهي أنه يمكن استخدام هذا التوثيق ضدك في حال تم القبض عليك). هناك نوعان من التوثيق:

- **مكتوب**. يتم تدريب رجال الشرطة على تدوين ملاحظات شاملة أثناء عملهم لأنه عند الشهادة في المحكمة يقول المثل "الأمر غير المكتوب، لم يحصل بتاتاً"، عليك إتباع نفس النصيحة وتدوين ملاحظات عن أي معلومات أو دليل وجدته سواء من أجل أهداف قانونية أو للرجوع إليه لاحقاً.
- **مصوّر**. عليك أيضاً أن تلتقط صوراً للمشهد بهدف جمع المعلومات وضمان عدم كشف العملية، إذا تم تغيير مكان أي شيء في الغرفة يجب إعادته إلى مكانه الأصلي، مع أن معظم الناس لا يتمتعون بالملاحظة القوية لكن هناك احتمال أن يلاحظ الهدف تغييراً ما في المكان. تعتبر كاميرات التصوير الرقمية وكاميرات الفيديو أدوات ممتازة لتوثيق الغرفة، لكن الكاميرات المستقطبة للضوء تقدم مزايا عديدة منها إمكانية إنتاج صورة فورية تمسكها بيدك وتستخدمها للمقارنة بين شكل الغرفة قبل وبعد التغيير.

بعد أن دخلت المبنى بنجاح وتوجهت إلى الطابق الرابع، ما هي الخطوة التالية التي يجب أن تتخذها، من أحد الاحتمالات ما يلي.

أول أمر ستفعله هو المرور عبر الممرات، لمعرفة إذا ما كان يوجد أحد ما في المكاتب، تجلس شريكتك على مقعد في منطقة الاستقبال وتتظاهر بأنها تقرأ مجلة، إذا ظهر الحارس في أحد جولاته ستخبره بأنها زوجتك وتنتظرك ريثما تحضر بعض الأوراق من المكتب، ومن ثم تجره في الحديث، إذا ظهر أحد ما من العاملين في المكتب ستخبره بأن مكتبك في الطابق الخامس وقد ضجرت من انتظارك وتبدأ تجول حول المبنى. في حالة أخرى سيفيدك وجودها بأنك ستكسب الوقت الذي تحتاجه لإنهاء ما تقوم به والخروج للبحث عنها، وتملك أيضاً مذياعاً صوتياً صغيراً في حقيبتها يخوّلك أن تسمعها في كل وقت.

لديك معدات فتح الأقفال، لذلك فأنت مستعد لاقتحام مكتب الهدف، لكن لن تحتاجها لأن معظم المكاتب ليست مقفولة، لذلك تدون هذه الملاحظة وأي ملاحظات أخرى حول نقاط الضعف التي اكتشفتها. تخرج كاميرا فيديو رقمية صغيرة من جيبك وتبدأ بالتسجيل موجهاً الكاميرا على رف الكتب الذي تنوي أن تفتشه.

جمع المعلومات

الهدف الأساسي لأي عمل حقيبة سوداء هو جمع المعلومات أو الأدلة بشكل سري. نناقش خلال بقية فصول هذا الكتاب عدداً من الطرق لتحقيق ذلك وخاصة إذا كنت تملك وصولاً فيزيائياً للحاسب. كجزء من الخطة التي وضعتها، عليك تحديد هدف العمل وفيما إذا كنت تبحث عن نمط محدد من المعلومات أو تقوم برحلة استكشافية للبحث عن شيء ما قد يكون مفيداً.

بما أنه من السهل جداً نسخ ملفات الحاسب، لذا عليك أن تحضر معك عدة وسائط تخزين لنسخ أي شيء تجده مهماً. يمكن أن تتراوح وسائط التخزين هذه من قرص صلب كامل لإنشاء صورة طبق الأصل عن أقراص الهدف إلى أقراص مرنة أو اسطوانات مضغوطة لنسخ ملفات متفرقة.

حتى لو كنت تتجسس حاسبياً، ليس عليك التركيز فقط على الحاسب كمصدر وحيد للمعلومات. ابحث في الغرفة بكاملها وعلى المكتب عن أوراق قد تحتوي كلمات مرور أو أي معلومات دقيقة أخرى. يجب توثيق أي شيء تجده، بعض الأماكن الأخرى التي قد تتضمن معلومات مفيدة:

- سلات المهملات (في المكتب وفي الخارج)
- دروج المكتب
- خزائن لحفظ الملفات
- ألواح الكتابة
- ألواح الفلين
- التقويم الجداري
- منظّم المواعيد

لقد وجدت حاسب الهدف يعمل مع شاشة التوقف الظاهرة على الشاشة. تحرك الفأرة ويظهر سطح المكتب الخاص بنظام التشغيل Windows Me، هناك ملف مفتوح يصف برنامج تدريب لإعادة بيع منتج بعد ستة أشهر من الآن. تلاحظ وجود قطعة ورق ملصقة على الشاشة مع

كلمة مرور، تخرج عدداً من الأقراص المرنة من حقيبتك وتبدأ بنسخ عدد من الملفات التي تبدو مهمة بينما تبحث في درج المكتب غير المقفول. ثم تقوم بتدوين الملاحظات عن أي شيء تجده وكل شيء قمت بفعله.

إزالة جميع الآثار والخروج

بعد أن حصلت على المعلومات المطلوبة، حان وقت ترتيب المكان وإزالة آثار العملية. هذا يعني أنه مهما كان المكان الذي قصدته يجب أن يترك كما كان عند دخولك إليه، وهنا تظهر أهمية التوثيق المصوّر لأن ذاكرة الإنسان معرّضة للخطأ وخاصة في ظروف مجهدة.

يجب أن تأخذ بالحسبان كل الأشياء التي جلبتها معك، إذا استخدمت برنامجاً على حاسب الهدف من قرص مرن أو اسطوانة مضغوطة لفحص أو نسخ محتوياته، تأكد من إزالته من السواقة، يستخدم بعض الجواسيس قوائم تدقيق لكل الأشياء التي بحوزتهم من أجل ضمان عدم ترك أي شيء في المكان والذي يمكن أن يثير الشكوك.

المرحلة الأخيرة من عمل الحقيبة السوداء هي الخروج بنجاح. حيث أن الخروج من مسرح الجريمة خطر بمقدار الدخول إليه، ومن الهام جداً الحفاظ على مستوى عالي من الحذر خلال العملية بأكملها.

لقد جمعت ما يكفي من المعلومات التي تدل على ضعف إجراءات الأمن الفيزيائية للمكاتب. إذا نجح أحد ما يعمل لصالح شركة منافسة في الدخول إلى المكتب سوف تكشف الكثير من المعلومات المهمة. تقوم بمشاهدة فلم الفيديو الذي صورته على شاشة كاميرا الفيديو وتتأكد من أن كل شيء في مكانه، ثم تتأكد مرتين من قائمة التدقيق وترى أن دفتر ملاحظاتك، القلم، كاميرا الفيديو، خمسة أقراص مرنة، وأسطوانتين مضغوطتين جميعها في الحقيبة، ثم تخبر شريكتك أنك قد انتهيت وقادم لأخذها.

لقد قدرت الوقت الذي ستستغرقه في المكتب بثلاثين دقيقة لكنك أنجزت مهامك في عشرين دقيقة، ثم تتصل بزميلك الذي يراقب خارج المبنى عن طريق الراديو وباستخدام كلمة سرية وتخبره أنك تتجه مع شريكتك إلى المصعد ومن ثم إلى السرداب. تلتقي مع زميلك على بعد شارع من المبنى وتتجهون جميعكم إلى المكتب حيث تقوم بمراجعة كاملة للمعلومات. لاحقاً تمر إلى النادي الصحي وتسلّم بطاقة الدخول إلى مكتب المفقودات قائلاً أنك وجدتها في الخزانة.

ثم تبدأ بإعداد تقرير حول جميع نقاط الضعف التي اكتشفتها، بما فيها كلمات المرور الملصقة على شاشات الحواسب، الحواسب المتروكة في حالة تشغيل مع ملفات هامة مفتوحة، وأبواب

المكاتب وخزائن لحفظ الملفات التي تترك دون قفل. تقوم بطباعة ملفات التدريب التي وجدتها لتستخدم كدليل، وبالطبع سيكون مديرك مسروراً بعملك.

الإجراءات المضادة

ماذا تفعل لمقاومة أعمال الحقيبة السوداء؟ سوف نلقي نظرة من خلال هذه الفقرة على الإجراءات المضادة العامة التي يمكن أن تطبقها. (نفصّل من خلال باقي الفصول مفهوم الإجراءات المضادة، لكن بما أن الأمن الفيزيائي هو موضوع واسع جداً لذلك فهذه الفقرة تصورية بجوهرها. سوف نزوّدك بعدد من الروابط على شبكة الإنترنت لتفاصيل أكبر).

أحد الأخطاء الأمنية الشائعة التي يمكن أن يرتكبها مدير النظام هو الدعم الكبير لحماية شبكات الحواسب وبالمقابل إهمال الحماية الفيزيائية التي قد تقود إلى هجوم فيزيائي. إذا كنت تعتقد، في تقرير الخطر الخاص بك، عن وجود تهديد ممكن لعمل الحقيبة السوداء والذي يمكن أن يكشف معلومات بالغة الدقة، فمن الضروري جداً أن تتخذ تدابير لتعزز الأمن الفيزيائي لموقعك. حتى لو لم تعتقد أنك ستكون هدفاً لعمل الحقيبة السوداء، فمن المفيد التدريب على إدارة اختبار للاختراق في وجه إجراءات الأمن الفيزيائي التي لديك لمعرفة الثغرات الموجودة.

الأمن الفيزيائي

يمكن أن نعرّف الأمن الفيزيائي بأنه أي شيء يقي المساحة التي تحوي الحاسب، وسائل التخزين، أو التجهيزات الشبكية (الكابلات، الموجّهات Routers، المبدّلات Switches) من الكوارث الطبيعية، الظروف البيئية (الحرائق، الفيضانات، والأعاصير)، الحوادث، الأعمال التخريبية، والتجسس. فيما يتعلق بالتجسس، تهدف الإجراءات الأمنية الفيزيائية إلى ما يلي:

- **الإعاقة**. وهو أي إجراء يمنع وقوع اقتحام مثل حارس، كاميرا مراقبة، الإضاءة، أو أي شعار يقول أن البناء محمي بجهاز إنذار. وتعتمد فعالية الإجراء على مدى تصميم الجاسوس على الدخول.
- **الكشف**. وهو أي إجراء يكشف عن عملية اقتحام، مثل حساسات مع إنذار، كاميرا مراقبة، أو حارس يفحص بطاقات الهوية عند المدخل.
- **الدفاع**. وهو أي إجراء يمنع أو يعيق المقتحم من تحقيق الدخول، مثل الأقفال، الأبواب المدعمة، أو إنذار يمكن سماعه بوضوح. أما فيما يتعلق بالإجراءات المضادة، فالوقت لصالحك وكلما استطعت أن تعيق الهجوم كلما زادت فرصة استسلام منافسك أو القبض عليه.

اعتماداً على الأهداف الثلاثة السابقة، تصنف الإجراءات الأمنية الفيزيائية إلى عدة فئات:

- **التحكم بالوصول.** وهو إجراء أمني يحد من الوصول إلى خدمة أو مواقع ضمن الخدمة إلى أشخاص محددين. يمكن أن يتكون نظام التحكم بالوصول من بطاقات الهوية، شارات، أجهزة القياس الحيوية مثل ماسحات البصمات، وأجهزة لقراءة البطاقات (المداخل التي تفتح باستخدام "بطاقة دخول" التي تصدر ترددات الراديو بالقرب من القفل).
- **التصميم المعماري.** تزيد عناصر تصميم المبنى الأمن (مثلاً، الأبواب المدعمة، الجدران الممتدة فوق الأسقف، الأنابيب الهوائية الصغيرة بحيث لا يمكن العبور عبرها، وتوجيه كابلات الاتصالات بحيث لا يمكن أخذ فروع منها بسهولة).
- **أنظمة الأمن الإلكترونية.** تزودنا هذه الأنظمة بإنذار مبكر عن وقوع اقتحام. هذه الأنظمة مصنوعة من حساسات (مثل حساسات الحركة، مبدلات مغناطيسية، أو حصائر ضغط) والتي تتقاطع مع الإنذارات. يمكن أن يكون التنبيه من النظام مسموعاً مثل صوت جرس أو صفارة للإنذار، أو ساكناً حيث يتم تنبيه قسم الشرطة أو شركة أمن خاصة. يمكن استخدام أنظمة التلفاز ذو الدارة المغلقة لمراقبة المواقع الهامة من المبنى.
- **الحراس.** وهم موظفون يلبسون لباساً رسمياً موحداً يخدّمون المداخل الرئيسة، يراقبون أنظمة الأمن، ويقومون بجولات حول المبنى.
- **الإضاءة.** وتتضمن الإضاءة الخارجية للمبنى والتي تنير نقاط الدخول للمبنى، وتصعّب بذلك إمكانية الدخول الليلي للجاسوس.
- **الأقفال وأنظمة المفاتيح.** تتضمن هذه الأنظمة تثبيت وصيانة أجهزة الأقفال الأمنية للمبنى ومداخل الغرف، بالإضافة إلى الحاويات (مثل، خزانة لحفظ الملفات، دروج المكتب، والخزنات).
- **الحوامل الواقية.** وهي إجراءات أمنية، مثل السياج أو البوابات والتي تشكل منطقة أمنية خارجية للمبنى.

تستخدم هذه الإجراءات الأمنية الفيزيائية ضمن مزيج متنوع لتشكيل نظام أمني متكامل. الأمن الفيزيائي مكلف، ومن المهم إنجاز تقرير بالخطر وتحديد نسبة الكلفة بالنسبة للفائدة والتي تتماشى مع نمط محدد من الإجراء الأمني قبل أن تستخدمه.

من الجدير بالذكر أن تقضي بعض الوقت لتحديد فيما إذا كانت الأنظمة الأمنية الفيزيائية التي لديك ملائمة، هذا لا يطبق على الحماية من التجسس فقط إنما على التدابير الأخرى أيضاً مثل مخططات الاسترداد بعد الكوارث، مخططات احتياطية، والتخزين البعيد عن الموقع. (إذا كنت

من مستخدمي خدمة التخزين البعيد عن الموقع، فتأكد من أنها مؤمنة جيداً لأنها قد تشكل هدفاً أسهل بكثير من موقعك الأصلي).

إذا كنت لا تملك خبرة كافية بالأمن الفيزيائي، فيما يلي بعض المواقع المفيدة على الإنترنت:

- **American Society for Industrial Security (ASIS)**. المجتمع الأمريكي للأمن الفيزيائي هو الاتحاد التجاري الرئيسي للمحترفين المرتبطين بالأمن المشترك. لمعلومات إضافية عن الاتحاد ASIS بالإضافة إلى مجموعة من المقالات الممتازة عن قضايا الأمن المختلفة، قم بزيارة الموقع، www.asisonline.org.
- **دليل المشترين للصناعات الأمنية**. ويمثل دليلاً شاملاً منشوراً من قبل الاتحاد ASIS ويتضمن لوائح عن أي منتج أو خدمة للأمن الفيزيائي يمكن أن تخطر على بالك. يتوفر إصدار هذا الدليل بالنسختين المجانية والمطبوعة على الموقع، www.sibgonline.com.
- **الأمن الفيزيائي FM 3-19.30**. وهو كتيب يدوي لحقل من حقول الأمن الفيزيائي الذي أصدره الجيش مؤخراً. إذا كنت تستطيع أن تفهم بعض الاختصارات، فإنه يمكنك تطبيق الكثير من المفاهيم والتقنيات الأساسية في المجتمع المدني. وهو متوفر على الرابط www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/toc.htm. (لقد أزال الجيش والحكومة مواقع ويب مختلفة والتي بدت أنها تشكل أخطار أمنية قومية، لذا قد تحتاج أن تعود للذاكرة المخبئية لموقع Google إذا لم يعد الموقع متوفراً).
- **برنامج الإغلاق الخاص بوزارة الدفاع**. يزود هذا البرنامج الجيش والحكومة بالمواصفات والمعلومات الأخرى عن الأقفال ومكونات الأمن الفيزيائي. اتبع الرابط http://locks.nfesc.navy.mil.
- **متطلبات الأمن الفيزيائي لتسهيلات مواقع المعلومات الحساسة**. وهو مستند عام للأمن الفيزيائي تابع لوكالة الأمن الوطنية والذي تسرب من خلال الإنترنت. المستند قديم بعض الشيء لكنه يحتوي على بعض المعلومات المفيدة عن الأمن الفيزيائي غير المألوف، يتوفر المستند على الرابط www.cryptome.org/nsa-scif.htm.

سياسات الأمن

إذا اضطررت لاختيار إجراء أمني واحد فقط لتأمين الحماية من أعمال الحقيبة السوداء أو من أي تهديد تجسسي، فماذا يكون؟ الإجراء الأمني الأكثر فعالية هو سياسة أمنية مكتوبة، مع أنها قد تبدو مضجرة.

السياسة هي مجموعة واضحة وشاملة ومعرفة بشكل حسن من المخططات والقواعد والتدريبات - أي تلك التي ترتبط بالمعلومات الأمنية. بالرغم من أن السياسات السيئة هي سمة مميزة غالباً للأجهزة الإدارية الحكومية العديمة الفعالية والمتقيدة بالأحكام، إلا أن السياسات المنظمة جيداً والتي يطبقها الموظفون بإخلاص هي جدار دفاعي قوي وفعال ومنظم ضد سرقة المعلومات.

فعلى سبيل المثال، يجب أن تعلن السياسة الأمنية عن مجموعة من التعليمات التي يجب على الموظفين إتباعها مثل محي ألواح الكتابة بعد الاجتماعات، عدم ترك المستندات الهامة على المكاتب، تمزيق الأوراق السرية، إقفال الخزانات ودروج المكاتب، استخدام تشفير قوي، واستخدام شاشات توقف محمية عند ترك الحواسب تعمل ودون رقيب.

الحالتان اللتان تفشل بهما جميع سياسات الأمن تقريباً هما رشوة وإرغام الموظفين، عليك أن تضمن فهم الموظفين التام للتدابير الأمنية، سوف يتعرض عملهم للخطر نظرياً إذا لجأ منافس غير أخلاقي إلى التجسس الاقتصادي وأذى أعمال الشركة. والشيء المهم أيضاً هو ضمان تطبيق السياسة الأمنية بقوة، وإلا فإنها ستفقد فعاليتها تماماً وينتهي بك الأمر بهدر وقتك وأنت تعمل على تطويرها. وإذا لم تقم بتطبيق سياسة بشكل جيد وقمت في نهاية الأمر بطرد أحد الموظفين لقيامه باختراق أمني، كانت قد منعته السياسة، فمن المحتمل جداً أنه كان يمكن تفادي هذا الموقف.

إن كتابة السياسة هي فن وعلم معاً، وعليك استخدام طاقم خبير لتطوير السياسات. فيما يلي بعض المصادر التي قد تعطيك بعض الأفكار العامة حول تشكيل سياسة أمنية:

- **وقاية تقنياتك**. مقالات عملية للأمن التعليمي الإلكتروني. تم إنتاج هذا الكتاب التمهيدي عن الأمن والمكتوب بلغة واضحة والموجه لمدراء إدارة التعليم والمدراء، من قبل المركز الوطني لإحصائيات التعليم (يمكنك استخدام هذا الدليل كمرجع لزملائك غير التقنيين). اتبع الرابط للحصول على نسخة إلكترونية /http://nces.ed.gov/pubs98/safetech.
- **الكتيب اليدوي لبرنامج الأمن الصناعي الوطني (NISPOM)**. يتضمن هذا الكتيب جميع المتطلبات، القيود، التصنيفات، والإرشادات لمنع كشف المعلومات السرية من قبل مصادر ممنوعة. بالرغم من أن هذا الكتيب مخصص للوكالات الحكومية والمتعهدين، إلا أنه لا بد من قراءته من قبل أي شخص مهتم بحماية شيء ما من نشاطات التجسس. يمكنك تحميل هذا الكتيب من الموقع، www.dss.mil/isec/nispom.htm.
- **الكتيب الأمني الخاص بوكالة الأمن الوطني**. لقد تمت طباعة الكتيب فرضياً من جديد من نسخة مصورة له ومن ثم تسرب عبر الإنترنت. يبدو الكتيب حقيقياً ويمثل نموذجاً جيداً لكيفية خرق سياسة أمنية في أي حالة من الحالات، وهو متوفر على الرابط .www.cl.cam.ac.uk/ftp/users/rja14/nsaman.pdf

- **دليل أمن المواقع (RFC2196)**. تطبيق مهام أمن المواقع (Internet Engineering Task Force (IETF. وهو دليل تطبيق مهام هندسة الإنترنت من أجل تطوير السياسات الأمنية للحواسب وإجراءات للمواقع التي تملك أنظمة متصلة بالإنترنت، يمكنك تحميلها من الرابط ftp://ftp.isi.edu/in-notes/rfc2196.txt.

خطر: السفر إلى الخارج

رغم أن الشركات الكبرى تتبع سياسات أمنية، إلا أنه لا يمكن تطبيق هذه السياسات عند السفر إلى خارج الولايات المتحدة. عليك أن تدرك أن عدداً من الحكومات الأجنبية تقوم برعاية عمليات التجسس الاقتصادي ضد المسافرين الأجانب. قد تكون هذه العمليات مدبرة ومنفذة بطريقة بشعة - مثلاً، غرف الفنادق التي تم تفتيشها والحواسب المتروكة التي تم فحصها. يقدّم المدير التنفيذي للجنة مكافحة التجسس الوطني الحكومي (www.ncix.org) مجموعة من النصائح لحماية المعلومات الخاصة بالمسافرين من أجل العمل إلى الخارج:

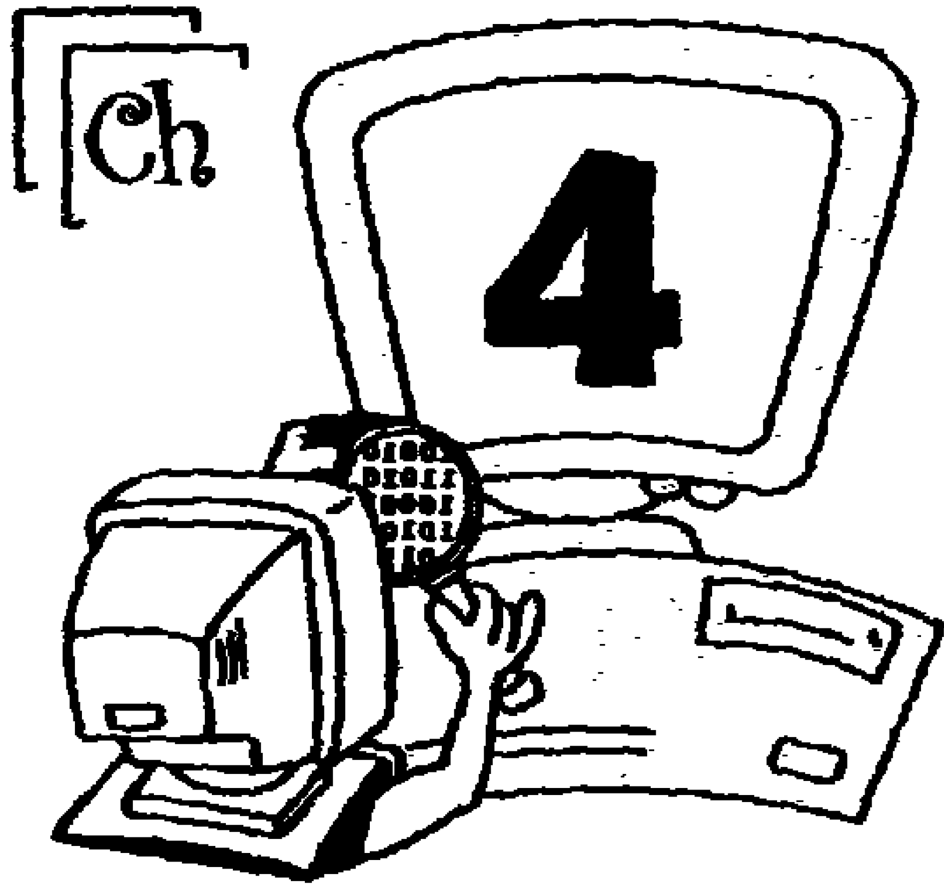
- احتفظ بجميع المستندات بالغة الدقة بحيازتك الشخصية في جميع الأوقات.
- غرف الفنادق والمطاعم هي أماكن غير مناسبة لإجراء محادثات حساسة. حاول أن تدير لقاءاتك في الخارج في أماكن لا تتعرض فيها إلى المضايقة أو أن حديثك لا يمكن أن يسمع بالصدفة.
- عليك إدراك أن حاسبك المحمول هو هدف أساسي للسرقة. إذا اضطررت إلى أن تأخذه معك احتفظ به مع الأمتعة المحمولة باليد، لا تمرره مع باقي الأمتعة. تركه في غرفة الفندق أو خزانة الفندق يشكل خطراً كبيراً أيضاً، وفي حال اضطررت إلى أن تتركه في غرفتك قم بإقفاله في حقيبة سفرك بحيث يكون بمنأى عن الأنظار بينما تكون نائماً أو في الخارج. وإذا احتاج الأمر قم بنسخ الملفات الهامة إلى قرص مرن، أسطوانة مضغوطة، أو قرص خارجي ثم احذفه من القرص الصلب الأساسي قبل السفر. احتفظ بوسائل التخزين معك، وبعيداً عن حاسبك الشخصي.
- إذا توفرت لديك تجهيزات للاتصالات الآمنة فعليك استخدامها لأي نقاش بالأمور شديدة الحساسية. لا تستخدم الحاسب أو الفاكس في الفنادق الأجنبية أو الأعمال للأمور شديدة الحساسية.
- استخدم التشفير لحماية الملفات والمجلدات شديدة الحساسية.
- استخدم برنامج "حذف" الملفات لحذف الملفات بشكل آمن، في حال تمت سرقة الحاسب المحمول لا يمكن استعادة الملفات المحذوفة.

- قم بحماية أي مواد غير مرغوبة بالغة الدقة، حتى تتخلص منها بأمان عن طريق حرقها، أو قطعها، قم بتمزيق القرص المرن إلى قطع صغيرة.

تلخيص

يركز معظم الناس على أمن الشبكات ويتجاهلون كلياً أن الجاسوس الذي يخترق الأمن الفيزيائي يستطيع بسهولة كبيرة أن يحصل على المعلومات البالغة الدقة. في الواقع، يشكّل المتنصت الذي يملك وصولاً فيزيائياً إلى الحاسب خطراً أكبر من جاسوس يقتحم عبر شبكة غير مؤمنة وذلك لأنه يستطيع أن يطّلع على المعلومات المخزنة على الحاسب بالإضافة إلى المستندات، الصور، وأشكال أخرى من المعلومات غير الرقمية.

تنفذ أعمال الحقيبة السوداء المعقدة عادة من قبل الوكالات القانونية، وكالات الاستخبارات الحكومية، الجيش، أو الأفراد المتورطون بأعمال التجسس الاقتصادي العالي المستوى. حتى لو لم تكن تعتقد أنك هدف ضمني لأحد هذه الجماعات، ما زال عليك أن تنتبه إلى أمنك الفيزيائي. إن الأساليب التي تستخدمها لتعزيز أمنك الفيزيائي ضد الجواسيس تحميك من المجرمين العاديين الذين لا يكونون مهتمين عادة ببياناتك لكن في بيع تجهيزاتك مقابل المال.



اختراق النظام

لا يعني اختراق الأمن الفيزيائي الذي يحمي الحاسب أنه بإمكانك كشف جميع أسراره، حيث تشكّل طرائق المصادقة Authentication[1] على مستوى النظام مثل كلمات المرور الخاصة بنظام الدخل/الخرج الأساسي BIOS عند بدء تشغيل الحاسب وعملية تسجيل الدخول لنظام التشغيل Windows، حاجزاً صلباً أمام جاسوس مهتم بالحصول على المعلومات.

بالرغم من النوايا الصالحة لبائعي التجهيزات والبرمجيات، توجد عدة طرق لاختراق النظام الحاسبي، وهذا هو ما سنتحدث عنه في هذا الفصل. سوف تتعلم نقاط الضعف على مستوى النظام والأدوات والتقنيات لاستغلالها (بعضها يتطلب استخدام مفتاح للباب، وأخرى تتطلب خلع الباب)، كما ستتعلم بعض الإجراءات المضادة الأساسية التي يمكنك استخدامها "لتقوية" حاسبك ضد المتنصتين المهتمين بمحتويات حاسبك.

أساليب الجواسيس

في هذا الفصل، ستتنكر بهيئة عميل KGB يمر بأوقات صعبة، (تقنياً، تم انحلال KGB مع انهيار الاتحاد السوفييتي عام 1991، وقام الرئيس الأول لمجلس الإدارة في KGB، والذي يعتبر مسؤولاً عن التجسس الأجنبي، بتغيير اسم KGB (Komitet Gosudarstvenoi Bezopasnosti) إلى الاسم SVR (Sluzhba Vneshney Razvedky)[2] أي خدمة الاستخبارات الأجنبية).

---

[1] المصادقة Authentication: يستخدم هذا المصطلح في أنظمة التشغيل متعددة المستخدمين (multiuser) أو الشبكات. وهو يمثل عملية يستطيع النظام من خلالها التأكد من صحة معلومات الدخول الخاصة بالمستخدم. فعملية المصادقة تتضمن مقارنة اسم المستخدم وكلمة المرور بلائحة من المستخدمين المفوضين بالدخول. فإذا عثر نظام التشغيل على اسم وكلمة مرور متطابقين، فعندها يمنح المستخدم حق الوصول إلى النظام ولكن ضمن نطاق محدود بلائحة المرخص به، والتي يحددها رقم حساب المستخدم.

[2] يشير الاختصار KGB باللغة الروسية إلى "Комитет Государственной Безопасноти" لجنة السلامة الحكومية، والاسم الجديد SVR يشير إلى "Служба Внешней Разведки" خدمة الاستخبارات الأجنبية.

لقد تدهورت المعنويات والأجور في الأعمال الحكومية العامة الروسية إلى الحضيض على مر السنين، وقد أخبرك زملائك عن توفر فرص عمل مغرية في القطاع الخاص، أنت متخصص بالتجسس الاقتصادي لصالح مجلس إدارة KGB/SVR (مسؤول عن الحصول على الاستراتيجيات الغربية، الجيش، والتقنيات الصناعية) وتم تدريبك للقيام بأعمال الحقيبة السوداء واختراق الأنظمة الحاسبية. وحين يخبرك صديقك عن مؤسسة تجارية أوروبية ضخمة تقوم حالياً بتوظيف أشخاص ذوي "مهارات أمنية"، تقوم من جهتك ببعض التحريات وتتلقى فوراً عرضاً بالعمل لتدريس مهنة التجارة لمتعاقدين مبهمين من فريق ثالث التي تقوم الشركة أحياناً باستخدامهم. وبالتأكيد الأجر يفوق أجر الدولة، بصفتك عقيد في الجيش كنت تكسب ما يقارب عدة مئات من الدولارات (الأمريكية) بالإضافة إلى ما كنت تستطيع أن تكسبه خارج عملك، تقدّم طلباً رسمياً بالاستقالة وبعد عدة أسابيع تكون في غرفة اجتماعات في مقاطعة الدفاع في باريس، تحاضر دزينة من الطلاب.

تستخدم الماتروشكا كوسيلة للشرح وتوضح أن أمن الحاسب هو مثل الماتروشكا[1]. للوصول إلى الطبقة الأعمق حيث تتوضع الأسرار عليك نزع الطبقات الأعلى بالدور، أحياناً وخلال قيامك بالعملية تجد أن الدمى الخارجية ملونة بطريقة مماثلة للدمى الداخلية (وهي طريقة روسية غير واضحة للقول أن كلمات المرور المستخدمة للمصادقة على مستوى النظام قد تستخدم نفسها لحماية أنواع أخرى من المعلومات). بعد أن تضع الدمية جانباً تقول أن موضوع درس اليوم هو الطبقتان الخارجيتان للنظام الأمني للحاسب، كلمة المرور الخاصة بنظام الدخل/الخرج الأساسي BIOS وعملية المصادقة لنظام التشغيل.

استغلال نقاط الضعف

قبل أن تتمكن من استغلال نقاط الضعف للطبقات الأمنية الخارجية، عليك أن تكون على إطلاع كافٍ عنها، يتضمن ما يلي:

- **التعرّف على نظام الدخل/الخرج الأساسي BIOS**. عليك أن تعرف نوع ورقم إصدار نظام الدخل/الخرج الأساسي BIOS بسبب اعتماد بعض الأدوات والتقنيات على هذه المعلومات. يتم عادة عرض مصنّع BIOS ورقم إصداره على الشاشة، عند تشغيل الحاسب، مع نوع المعالج والذاكرة، وفي حال لم يتم عرض هذه المعلومات عليك الدخول إلى برنامج الإعداد BIOS (إن لم يكن محمياً بكلمة مرور) لاستعراض المعلومات. تضغط بشكل مستمر على

[1] الماتروشكا هي دمية روسية تقليدية متداخلة حيث تتضمن كل دمية خشبية دمية أصغر بداخلها.

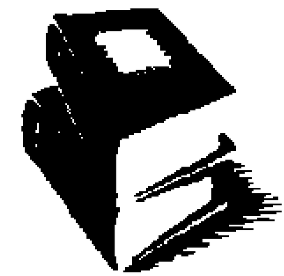
أحد أزرار لوحة المفاتيح مثل الزر Del، أو مجموعة مختلفة من الأزرار لتدخل إلى برنامج الإعداد عند تشغيل الحاسب، تتنوع هذه الأزرار بحسب المصنّع. بالإضافة إلى برنامج الإعداد عليك معرفة مصنّع الحاسب ونوعه.

- **التعرّف على نظام التشغيل.** تملك الإصدارات المختلفة من نظام التشغيل Windows نقاط ضعف مختلفة، كما لبرنامج BIOS، لذلك يجب معرفة إصدار نظام التشغيل الذي يعمل عليه حاسب الهدف. تستطيع معرفة إصدار نظام التشغيل من ملاحظة شاشة البدء التي تظهر قبل تحميل النظام أو قبل ظهور سطح المكتب.

مع الحصول على هذه المعلومات تذكر أنه عندما تهاجم حاسباً فإنه يكون في إحدى حالتين إما يعمل أو لا يعمل، لذلك اعتماداً على حالة الحاسب سوف تستخدم أدوات وطرائق مختلفة لاختراقه.

كلمات المرور الخاصة بنظام الدخل/الخرج الأساسي BIOS

يمثّل نظام الدخل/الخرج الأساسي شيفرة مكتوبة باستخدام لغة منخفضة المستوى على رقاقة متوضعة على اللوحة الأم وتتحكم بلوحة المفاتيح، العرض، محركات الأقراص، الاتصالات التسلسلية، وعدداً من الوظائف الأخرى. *(لغة منخفضة المستوى: اللغة التي تعتمد على الآلة أو اللغة التي تحوي نماذج بيانات وتعليمات تحكم قليلة، حيث تقابل كل تعليمة من تعليماتها تعليمة واحدة في لغة الآلة). تخزّن معلومات النظام BIOS مثل التاريخ، الوقت، ومعلومات إعداد النظام ضمن الذاكرة CMOS (Complementary Metal Oxide Semiconductor)، تتوضع عادة في رقاقة ساعة الزمن الحقيقي RTC (Real Time Clock) للحاسب.



لمعلومات أكثر عن نظام الدخل/الخرج الأساسي BIOS، قم بزيارة الموقع، www.wimsbios.com.

أساليب: إقلاع محطة الربط المزدوجة

من المفيد جداً فهم تسلسل عملية الإقلاع للحاسب، التي تتضمن الخطوات التالية:

1. **يقرأ المعالج الشيفرة من رقاقة BIOS، مما يؤدي إلى تشغيل مجموعة من الاختبارات (تدعى POST، اختبار ذاتي عند الإقلاع Power On Self Test) والتي تضمن أن أجهزة النظام تعمل بشكل صحيح. خلال عملية الاختبار POST يقوم نظام BIOS بما يلي:**

- يهيئ تجهيزات النظام (المكونات الصلبة للنظام Hardware) وسجلات الرقاقات.
- يهيئ إدارة الطاقة.
- يفحص ذاكرة الوصول العشوائي RAM.
- يفعّل لوحة المفاتيح.
- يفحص المنافذ التسلسلية والتفرعية.
- يهيئ محركات الأقراص المرنة ووحدات التحكم بمحرك القرص الصلب.
- يعرض معلومات النظام.

2. يقارن النظام BIOS بيانات تكوين النظام خلال الاختبار الذاتي مع المعلومات المخزنة في الرقاقة CMOS، (يتم تحديث الرقاقة CMOS عند إضافة مكونات جديدة للنظام).
3. بعد الانتهاء من العملية POST، يبحث النظام BIOS عن برنامج إقلاع ليحمّل نظام التشغيل، يبحث النظام عادة في سواقة الأقراص المرنة :A ومن ثم في القرص الصلب :C (يمكن تغيير هذه الإعدادات).
4. في هذه اللحظة، يسحب تسلسل الإقلاع المسؤوليات من النظام BIOS إلى النظام Windows، والذي يحمّل معلومات تكوين النظام Windows وبرامج تشغيل الأجهزة (متضمناً شيفرة مصادقة تسجيل الدخول في الأنظمة Windows NT/2000/XP).

إذا تمت عملية تسلسل الإقلاع بنجاح يتم تحميل وتشغيل برامج بدء التشغيل.

يوجد خياران لمصداقية الأمن على الأقل ضمن نظام BIOS، والتي يمكن تفعيلها في برنامج الإعداد عند بدء تشغيل الحاسب. وتتضمن ما يلي:

- **كلمة المرور عند الإقلاع**. يتم طلب كلمة مرور عند بدء تشغيل الحاسب قبل أن تتم متابعة عملية تسلسل الإقلاع. تسمى كلمة المرور هذه أيضاً بكلمة مرور المستخدم.
- **كلمة مرور برنامج الإعداد BIOS**. يتم طلب كلمة مرور للدخول إلى برنامج الإعداد لتغيير الإعدادات مثل إدارة الطاقة، دعم محرك القرص الصلب، والوقت والتاريخ. تسمى كلمة مرور هذه أيضاً بكلمة مرور المشرف Supervisor.

يتم تخزين كلمات المرور ضمن الرقاقة CMOS، مع باقي وسطاء النظام BIOS.

بالرغم من أن كلمات المرور الخاصة بالنظام BIOS هي إجراء أمني جيد، إلا أنها ليست فعالة ضد متنصت محترف. قد تجعل كلمات المرور الخاصة بالنظام BIOS المتطفلين بعيدين عن حاسبك، لكنها عائق صغير أمام شخص مزود بالأدوات والمعلومات الصحيحة.

تسأل طلابك عن الطرائق التي يمكن أن يستخدموها لاختراق نظام محمي بكلمات المرور الخاصة بالنظام BIOS، تتلقى بعض الإجابات وتبدأ بتوضيح وسائل الهجوم المختلفة التي كنت قد استخدمتها في الماضي.



تتضمن بعض وسائل اختراق كلمات المرور الخاصة بالنظام BIOS أساليب متعلقة بالمكونات الصلبة للحاسب. فإذا لم تكن تملك الخبرة الكافية لفتح الحاسب وتبديل مكوناته الداخلية، فحاول أن تتعلم الأساليب البرمجية بدلاً من ذلك. قد تقوم الكهرباء الساكنة والحماس المندفع بتخريب المكونات الإلكترونية بسهولة، حتى تعديل نظام BIOS باستخدام أدوات برمجية قد يسبب نتائج غير متوقعة إذا لم تأخذ حذرك.

الاستكشاف تبدأ محاضرتك بإخبار الطلاب أن أحد الأمور الأولى التي يجب أن تنجزها بصفتك جاسوس، في عمل الحقيبة السوداء أو أي نوع من النشاط الجاسوسي، هو استكشاف هدفك. يتضمن هذا الاستكشاف بالنسبة للحواسب مع كلمات مرور الخطوات التالية:

- قم بزيارة موقع الويب الخاص بمصنّع الحاسب الذي تريد مهاجمته لتعرف فيما إذا كانت هناك أي معلومات عن إلغاء تفعيل أو إعادة تحديد كلمة المرور.
- اتصل بالدعم الفني للمصنّع مباشرة وحاول الحصول على معلومات عن كيفية اختراق كلمة المرور. يسألك معظم المصنّعون أسئلة كثيرة ليعرفوا إذا كنت المالك الشرعي، لذا قد تحتاج لاستخدام مهاراتك في الهندسة الاجتماعية.
- قم بإجراء عملية بحث عن طريق محرك البحث Google عن الحاسب الذي ترغب بمهاجمته مثل كتابة الجملة التالية في مربع البحث "Dell latitude BIOS password"، قد يقودك هذا البحث إلى برامج خدمية أو بيانات تستطيع أن تستخدمها عند قيامك باختراق نمطاً محدداً من الحواسب.

سوف توفر عليك المعلومات التي جمعتها خلال طور الاستكشاف قدراً كبيراً من الوقت والجهد خلال مهاجمة نظام محمي بكلمة مرور خاصة بنظام الدخل/الخرج الأساسي BIOS.

كلمات المرور الخفية ليست كلمات المرور الخفية مؤامرة سرية، وطبع الإنسان أنه ينسى لذلك فإنه عمل سيئ أن يكون لديك زبون محجوز عن حاسبه الخاص لأنه نسي كلمة المرور. فلهذا السبب يعمد معظم مصنّعي نظام الدخل/الخرج الأساسي بوضع كلمات مرور خفية لمنتجاهم والتي تسمح لك أن تتسلل إلى نظام محمي بكلمة مرور لا تعرفها. كما يقدّم مصنّعو الحواسب غالباً كلمات مرور خفية خاصة بهم. (يزود مصنّعو النظام BIOS صانعي الحواسب ببرامج خدمية ليتمكنوا من تعديل إعدادات محددة لتتلاءم مع أنظمتهم). في حال وجود كلمة مرور افتراضية، تستطيع لاحقاً تغيير كلمة مرور المستخدم من خلال برنامج الإعداد، أو باستخدام برنامج يكشف كلمة المرور بعد تشغيل النظام Windows.

تعرض الجداول 4-1، 4-2، 4-3، و4-4 كلمات المرور الخفية الشائعة، مصنفة بحسب المصنّع، والتي تم استخدامها بنجاح لاختراق كلمات المرور لنظام الدخل/الخرج الأساسي BIOS.

قد تستهلك عملية تجريب كلمات المرور الخفية المختلفة كثيراً من الوقت، ولا توجد ضمانة لنجاح كلمات المرور الخفية هذه على حاسب محدد (جميع كلمات المرور الخفية مصممة خصيصاً لأنظمة سطح المكتب، وحالياً لا توجد لوائح بكلمات مرور خفية شائعة للحواسب المحمولة). كما يجب أن تتذكر أن بعض الأنظمة قد تتضمن ميزات أمنية إضافية، فعلى سبيل المثال تقوم بعض منتجات شركة Dell بقطع التغذية عن الحاسب بعد ثلاث محاولات فاشلة لإدخال كلمة المرور، مما يجعل عملية توقع كلمة المرور بطيئة ومتعبة جداً.

توقع كلمة المرور إذا لم تنجح طريقة كلمات المرور الخفية، توجد طريقة أخرى وهي بكل بساطة شديدة توقع كلمة المرور. اذهب إلى الفصل السادس لمعلومات حول توقع كلمة المرور ومعلومات تساعدك على مهاجمة النظام BIOS أو أي نوع آخر من كلمات المرور.

استعادة كلمة المرور لا تكون كلمات المرور للنظام BIOS محمية بتشفير قوي ويمكن كشفها بسهولة باستخدام الأدوات المناسبة. يمكنك باستخدام مجموعة من البرامج الخدمية، المعروضة ضمن فقرة "أدوات لاختراق النظام" من هذا الفصل، استعادة كلمة مرور للنظام BIOS إذا تم إقلاع الحاسب من قبل و هو في حالة العمل.

سحب القرص الصلب من إحدى الطرق السهلة للتغلب على كلمة مرور النظام BIOS والتي يمكن أن يستخدمها طلابك، هي ببساطة إزالة القرص الصلب من الحاسب المحمي وتركيبه في حاسب آخر. بما أن نظام الدخل/الخرج الأساسي هو جزء من اللوحة الأم، فسوف يتم تطبيق الحماية على ذلك الحاسب ولا يتعلق بقرصه الصلب أو أي وسائل تخزين أخرى. (توجد منتجات النظام BIOS، والمرتبطة بشكل خاص بالحواسب المحمولة الحديثة، والتي تحمي القرص الصلب أيضاً. إذا وجد هذا النوع من الأمن فلن تتمكن من استعراض البيانات على القرص بنقله إلى حاسب آخر).

الجدول (4-1): كلمات مرور Bios لشركة AMI

A.M.I	AAAMMMIII	Aammii	AM
AMI	AMIISW	AMI.KEY	AMI.KEZ
AMI?SW	AMI_SW	AMI~	AMIAMI
AMIDECOD	Amipswd	AMIPSWD	AMISETUP
BIOS	BIOSPASS	CONDO	HEWITT RAND
LKWPETER	PASSWORD		

الجدول (4-2): كلمات مرور Bios لشركة Award

?award	_award	01322222	01322222
256256	589589	589721	595595
598598	admin	Alfarome	ALFAROME
Ally	aLLY	ALLy	ALLY
APAf	award	Award	AWARD PW
AWARD SW	AWARD?SW	AWARD_SW	Awkward
AWKWARD	BIOS	Biosstar	Biostar
BIOSTAR	CONCAT	Condo	Condo
CONDO	d8on	Djonet	g6PJ
h6BB	HELGA-S	HEWITT RAND	HLT
j09F	j256	j262	j322
j332	J64	KDD	Lkw peter
Lkwpeter	Lkwpeter	LKWPETER	PASSWORD
Pint	PINT	SER	Setup
SKY_FOX	SWITCHES_SW	Sxyz	Syxz
SYXZ	SZYX	t0ch20x	t0ch88
TTPTHA	TzqF	Wodj	ZAAADA
Zbaaaca	ZBAAACA	ZJAAADC	

الجدول (4-3): كلمات مرور شركة Phoenix Technologies

Phoenix	PHOENIX	CMOS	BIOS

الجدول (4-4): كلمات مرور لمصنفين آخرين

Manufacturer	Password
Biostar	Biostar
Compaq	Compaq
Dell	Dell
Enox	xo11nE
Epox	Central
Freetech	Posterie
IBM and VOBIS	Merlin
IBM (Aptiva)	(Press both mouse buttons on boot up.)
Iwill	Iwill
Jetway	Spooml
Packard Bell	bell9
QDI	QDI
Siemens	SKY_FOX
TMC	BIGO
Toshiba	Toshiba

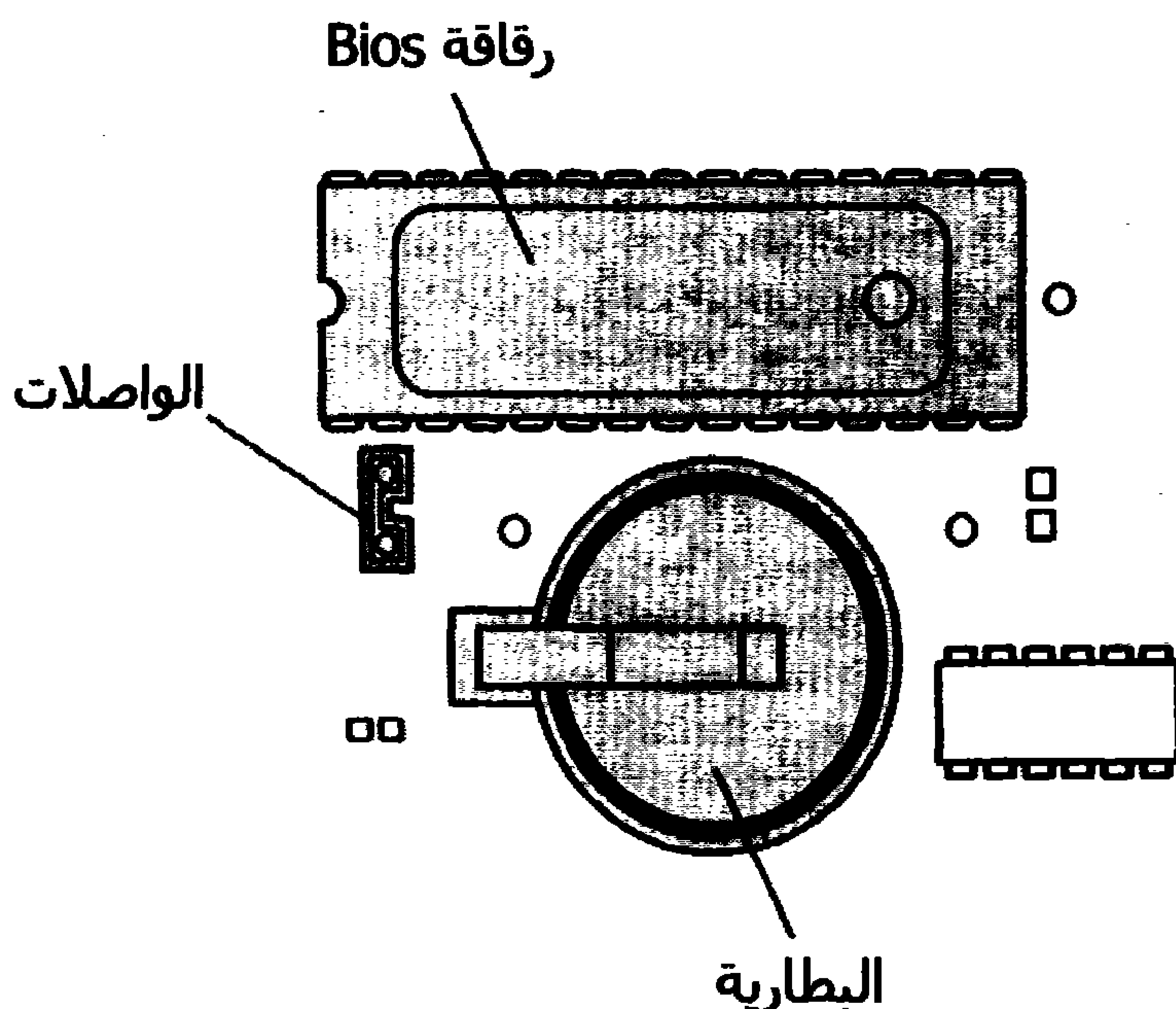
من الميزات الأخرى لنظام الدخل/الخرج الأساسي BIOS التي يجب أن تدركها، وخاصة الحواسب التي تعمل كملقمات، هي خيار "كشف الاقتحام الهيكلي Chassis Intrusion Detection"، إذا كان هذا الخيار مفعّلاً تظهر لك رسالة أثناء تسلسل الإقلاع إذا كان صندوق الحاسب مفتوحاً. وفي المستقبل سوف تكون الحواسب مندمجة مع تقنية ASF (Alert Standard Format)، في بيئات المشاريع الجريئة، وتتلخص في أن حاسب متصل بشبكة سوف يقوم بإرسال رسائل إلى طرفية

تحكم مركزية معلماً عن حالته. مثلاً، إذا فتحت صندوق الحاسب ليلاً لإخراج محرك القرص الصلب، سوف تتفاجأ بحراس الأمن فوقك بعد أن تسلموا رسالة الاقتحام الهيكلي إلى مكتبهم من نظام الدخل/الخرج الأساسي BIOS. (يمكن أن تتغلب على تقنية ASF بسحب كابل الشبكة أو قطع التغذية، لكن قد يؤدي هذا العمل نظرياً إلى إصدار إنذار آخر).

مسح رقاقة CMOS: من الوسائل الأخرى المتعلقة بالمكونات الصلبة للحاسب هي مسح الإعدادات المخزنة على الرقاقة CMOS. يتم تطبيق الإعدادات الافتراضية، إذا كانت معلومات النظام BIOS ناقصة أو تالفة، والتي لا تتضمن الحماية بكلمة مرور. يمكنك في الواقع التغلب على دائرة الأمن باستخدام كلمة مرور بوساطة تقنيتين (انظر إلى الشكل 1-4 لرؤية مكونات النظام BIOS المختلفة):

- **البطاريات Batteries**. تحتاج البيانات المخزنة ضمن رقاقة CMOS إلى طاقة تزودها بها عن طريق بطارية صغيرة. افصل التغذية الرئيسة عن الحاسب، ثم قم بتحديد بطارية الرقاقة CMOS وإزالتها (تبدو مثل بطارية الساعة مستديرة ومسطحة). بعض المصنّعون يقومون بلحام البطارية مما يصعّب الأمر عليك قليلاً إذا لم تكن تعرف كيف تفك لحامها. بعد إخراج البطارية سوف تُحذف جميع البيانات في الذاكرة بشكل نهائي، تستغرق عملية تفريغ البطارية من عدة دقائق إلى عدة أيام بحسب السعة في الدارة (طريقة سهلة وآمنة لتفريغ بطارية الرقاقة CMOS هو ملامسة مقاومة قيمتها 10k-ohm بروابط البطارية). عندما يتم إقلاع الجهاز يقوم برنامج BIOS بفحص إعدادات النظام للرقاقة CMOS، فلا يجد أية إعدادات، فيقوم باستخدام الإعدادات الافتراضية ويسجلها على رقاقة CMOS. إن سحب أرجل محددة من الرقاقة يؤدي أيضاً إلى حذف الإعدادات، عادة يمكنك من خلال وثيقة اللوحة الأم أن تتعرف على كيفية فعل هذا.

- **الواصلات Jumpers**. طريقة أخرى لتهيئة الرقاقة CMOS باستخدام الواصلة (زوج من الشوكات وهي نقاط اتصال كهربائية إلى اللوحة الأم تستخدم لتغيير إعدادات المكونات الصلبة) وتسمى "واصلة التحكم باختراق كلمة المرور." إذا تم تحريك الواصلة إلى الوضعية المقفلة يتم تغيير كلمة المرور لنظام الدخل/الخرج الأساسي BIOS عند تشغيل الحاسب في المرة القادمة. يتم عادة إلصاق لافتة على الواصلة مكتوب عليها "Clear CMOS ،Clear RTC، أو PWRD"، يختلف تكوين الواصلة باختلاف الحواسب، وهنا يأتي استكشافك عن حاسب الهدف ملائماً للاستخدام.



الشكل (4-1) رقاقة BIOS على اللوحة الأم في أعلى الشكل والبطارية التي تزود التغذية للإعدادات المخزنة في الرقاقة CMOS والواصلات لتهيئة الرقاقة CMOS.

يمكنك تطبيق هذه المهاجمات على التجهيزات الحاسبية في حالة كون الحاسب مطفئاً، أما إذا كان الحاسب قد أقلع ويعمل مسبقاً، يمكنك مسح الإعدادات المخزنة في الرقاقة CMOS باستخدام إحدى الطريقتين البرمجيتين:

- **استخدام برنامج لمسح الرقاقة CMOS.** أحد البرامج الخدمية التي تقوم باستعادة كلمات المرور الخاصة بالنظام BIOS بالإضافة إلى مسح بيانات الرقاقة CMOS، هو البرنامج Cmospwd والمفصل في فقرة "أدوات لاختراق النظام" من هذا الفصل.

- **تقنية BIOS الومضي.** معظم أنظمة الدخل/الخرج الأساسية BIOS قابلة للترقية عن طريق استخدام تقنية الذاكرة الومضية. تمسح الترقية الومضية إعدادات الرقاقة CMOS بالإضافة إلى ترقية النظام BIOS، انتبه عند استخدام هذه الطريقة لأن الوقوع بأي خطأ قد يؤدي إلى تلف اللوحة الأم.

السيئة الأساسية لتقنية مسح إعدادات الرقاقة CMOS هي أن المستخدم سيرتاب إذا اختفت كلمات المرور للنظام BIOS، عليك اللجوء إلى هذه الطريقة في حال لم تنجح أي طريقة أخرى.



إن العبث بإعدادات BIOS وCMOS ليست للجاسوس الجبان أو غير التقني لأنه يمكن أن تغير إعداداً ما بالخطأ والذي يجعل النظام غير قابلاً للاستخدام (لوقت مؤقت عادة). عليك أن تحتفظ بنسخة احتياطية، إذا أمكن ذلك، لمحتويات الرقاقة CMOS قبل أن تبدأ بتغييرها. يوجد عدد من البرامج الخدمية التي تحفظ وتستعيد إعدادات الرقاقة CMOS، والتي تظهر فائدتها بشكل خاص عندما تعبث بشيء ما دون قصد.

مواضيع تتعلق بنظام الدخل/الخرج الأساسي BIOS للحواسب المحمولة عليك تسليط الضوء على الحواسب المحمولة خلال محاضرتك فيما يتعلق بأمن BIOS. إن عملية كشف كلمة مرور لحاسب محمول أصعب بكثير من ابن عمه الحاسب المكتبي، توجد مجموعة من الأمور التي تعقّد الهجوم على نظام BIOS للحاسب المحمول وهي:

- **التصميم الهيكلي**. مع أن تعيين الواصلة وإخراج البطارية يؤدي إلى مسح كلمة مرور النظام BIOS، إلا أن عملية فتح الحواسب المحمولة والوصول إلى مكوناها المادية أصعب بكثير على الجاسوس العادي.
- **الذواكر EEPROMs**. تخزن معظم الحواسب المحمولة إعدادات النظام BIOS بما فيها كلمات المرور، ضمن ذاكرة قراءة فقط قابلة للبرمجة والمسح إلكترونياً (Electrically Erasable Programmable Read-Only Memory) بدلاً من الذاكرة CMOS. والآن لتتمكن من الوصول إلى وسطاء BIOS يجب عليك أولاً فك لحام الذاكرة EEPROM من اللوحة الأم ومن ثم قراءة محتوياها باستخدام قارئة PROM* (PROM هي ذاكرة للقراءة فقط قابلة للبرمجة). يحتاج هذا النوع من المهاجمة إلى مهارات وأدوات خاصة.
- **البطاريات**. إخراج البطارية من داخل الصندوق يمكن أن يهيئ كلمة المرور في بعض الحواسب المحمولة. لكن عليك أن تتذكر وجود نوعين من البطاريات: أحدها خاصة بالرقاقة CMOS (في حال وجودها) والأخرى تعمل كعازل للتغذية خلال عملية تبديل البطاريات للحاسب المحمول.
- **كلمات المرور الخاصة بمحركات الأقراص الصلبة**. يُضمِّن بعض المصنّعون كلمات مرور خاصة بمحرك القرص الصلب والتي تمنع تبديل محرك القرص الصلب إلى حاسب محمول آخر.

إذا كنت تعمل على أمن BIOS لحاسب محمول، عليك قضاء بعض الوقت لتستكشف الطرق المختلفة لاختراق النظام. يمكن التغلب على الأمن المتطور للحواسب المحمولة، توجد مجموعة من الطرائق لاختراق كلمات المرور وتختلف باختلاف المصنّع، نستعرض فيما يلي بعض الأمثلة:

- **التجهيزات الصلبة.** يستخدم مصنّعو الحواسب المحمولة أنماطاً مختلفة من التجهيزات الصلبة لتغيير كلمات المرور لنظام BIOS. مثلاً يمكن تغيير كلمات المرور لبعض أنواع الحواسب المحمولة من إنتاج الشركتين Toshiba وCompaq باستخدام جهاز "الحلقة العكسية"، وهو ببساطة وصلة من النوع DB-25 والتي تتصل بمنفذ الحاسب التفرعي. في بعض حواسب Toshiba إذا تم وصل الأرجل التالية – 1-5-10، 2-11، 3-17، 4-12، 6-16، 7-13، 8-14، 9-15، 18-25 – وكشف نظام BIOS هذا الإعداد خلال الإقلاع فيقوم بمسح كلمة المرور.
- **تركيبات لوحة المفاتيح.** يستخدم بعض المصنّعين تركيبات مختلفة للوحة المفاتيح لتجاوز الإعدادات الأمنية. مثلاً، تتجاوز معظم حواسب Toshiba المحمولة كلمة المرور إذا تم ضغط الزر Shift اليساري باستمرار خلال عملية الإقلاع.
- **الأقراص المفتاحية.** تستخدم بعض الأنواع القديمة لحواسب Toshiba المحمولة "قرص مفتاحي" لتغيير كلمة المرور. يتم تزويد مراكز خدمة المصنع بقرص مرن خاص يتم إدخاله ضمن محرك الأقراص المرنة للجهاز، ثم يقوم الخبير التقني بإقلاع الحاسب، اضغط زر الإدخال Enter عندما يطلب منك إدخال كلمة المرور ثم اضغط Y و Enter عندما يطلب منك تغيير كلمة المرور، ثم تظهر شاشة برنامج الإعداد BIOS، حيث يمكن إدخال كلمة مرور جديدة. لقد تبين أن القرص السحري لاستعادة كلمة المرور هو عبارة عن قرص مرن مهيأ مع تعيين القيم التالية للبايتات الخمسة الأولى من القطاع الثاني: 00 00 59 45 4B. يمكنك استخدام برنامج التحرير الست عشري (Hex Editor) لتقوم بإنشاء قرصك الخاص أو قم بالبحث عن برنامج يدعى KeyDisk والذي يقوم آلياً بإنشاء قرص لك.
- **خدمات الاستعادة التجارية.** يقدم العديد من مصنعي الحواسب المحمولة وقليل من المكاتب الخدمية خدمات لمالكي الحواسب المحمولة الذين لا يستطيعون الوصول إلى أنظمتهم لأي سبب كان. يبيع موقع تابع لمخربي كلمات المرور، (www.pwcrack.com) "رقاقات الأمن" والتي تستبدل تلك الموجودة في عدد من الحواسب المحمولة الشائعة، وبالتالي إعادة تغيير الأمن، ومن ثم يرسلون لك رقاقة مع الإعدادات الافتراضية لنظام BIOS الخاصة بحاسبك. كما يمكنك أيضاً إرسال الرقاقة لهم ويقومون باستخلاص كلمة المرور منها. تتخصص شركة Nortek Computers Ltd. (www.nortek.on.ca) بإزالة كلمات المرور الذكية عند التشغيل وكلمات المرور الخاصة بمحرك القرص الصلب، مع استعادة كاملة لبيانات القرص الصلب المحمي. الشركة الكندية مفرطة الشك وتطلب عقداً بالملكية قبل أن تقوم باسترجاع حاسب محمول محمي.

إجراءات مضادة: الحواسب المحمولة

تعد سرقة الحواسب المحمولة النوع الثاني الأكثر انتشاراً للاختراق الأمني المشترك من قبل الدخلاء. المال الذي يمكن أن يجنى من وراء بيع حاسب محمول يجذب معظم اللصوص، لكن الربح الأهم عندما تكون بيانات القرص الصلب هي الهدف. تكون سرقة الحواسب المحمولة غالباً مساراً سهلاً للحكومة، الجيش، أو الأسرار المتعلقة بالأعمال.

- تشير الإحصائيات وفق معهد الأمن الحاسبي ومكتب التحقيقات الفدرالي، أنه تمت سرقة 591,000 حاسباً محمولاً في الولايات المتحدة الأمريكية عام 2001، وعادة لا تتم استعادة نسبة 97% منها.
- صرح رئيس المفتشين في وزارة العدل خلال تقرير حديث له، "فقدت خمس وكالات، من بينها مكتب التحقيقات الفدرالي ووكالة مكافحة المخدرات DEA، 400 حاسباً محمولاً يتضمن أكثر من نصفها بيانات أمنية وطنية بالغة الدقة."
- اختفى حوالي 600 حاسب محمول من وزارة الدفاع البريطانية منذ عام 1997، ويتضمن بعضها معلومات حكومية وعسكرية بالغة الدقة.

نستعرض فيما يلي بعض الخطوات التي تجعل بيانات حاسبك المحمول بعيدةً كل البعد عن أيدي الجواسيس:

- لا تدع الحاسب المحمول يغيب عن ناظريك (إذا أحببت يمكنك ربطه بيدك).
- احفظ الحاسب المحمول في مكان آمن عندما لا تستخدمه.
- استخدم تشفيراً قوياً لحماية المعلومات البالغة الدقة كما هو مشروح في فقرة "الإجراءات المضادة" من الفصل الخامس.
- استخدم أكبر قدر ممكن من خيارات الأمن لنظام BIOS، بالرغم من أن هذا الإجراء لا يوفر الأمن التام لمنافس قوي، لكنه خط الدفاع الأول. (احتفظ بكلمات المرور في مكان آمن، حيث تمتلئ منتديات الإنترنت بحكايات الناس حول كلمات مرورهم الضائعة).

أنظمة التشغيل Windows 3.X/9X/ME

إذا كان أمن نظام BIOS هو الدمية الخارجية للماتروشكا، حالما تفتحها فسوف تواجه الدمية التالية وهي نظام التشغيل. بالرغم من إصدار شركة Microsoft نظام التشغيل Windows XP في خريف 2001، إلا أن نظام التشغيل Windows 98 كان ما يزال يحتل القيادة في نهاية عام 2002 كونه نظام التشغيل الأكثر استخداماً، وهذا أمر جيد للجواسيس لأن عائلة نظم التشغيل Windows 3.x/9.x/ME لا تتميز بالكثير من خصائص الأمن الموثوق.

الاعتماد على مربع الحوار الخاص بتسجيل الدخول في الإصدارات القديمة لنظام التشغيل Windows من أجل الحصول على الأمن هو أمر بغاية الذكاء مثل ذكاء شخص مطارد من قبل مصنّع الفودكا في موسكو ويشرب شراب الساموغون (فودكا مصنعة في البيت بطريقة غير مشروعة) في نفس الوقت. مع أنه كلا الأمرين قد يسببان الضرر لك على المدى البعيد من وجهة نظر اقتصادية.

إذا واجهت مربع الحوار الخاص بتسجيل الدخول في الأنظمة Windows 3.x/9.x/ME، فقم بإغلاقه بضغط زر "إلغاء الأمر Cancel" فقط، ثم يظهر سطح المكتب ولديك حرية الوصول الكاملة إلى النظام والملفات. تتلخص وظيفة مربع الحوار الخاص بتسجيل الدخول باستعادة مظهر سطح المكتب والاتصال بأي موارد شبكية اعتماداً على اسم المستخدم وكلمة المرور الخاصة به، يتم تخزين هذه الإعدادات في ملف التشكيل الجانبي[1] (PWL.).



لمعلومات أكثر عن التشكيلات الجانبية وكيفية استخلاص كلمات المرور المخزنة بداخلها، راجع الفصل السادس.

الإجراء الأمني الوحيد على مستوى النظام (غير المرتبط بالشبكات) في الإصدارات الأقدم لنظم التشغيل Windows هي شاشات التوقف المحمية بكلمات مرور، يستطيع المستخدم أن يعين كلمة مرور يجب إدخالها أثناء تشغيل شاشة التوقف للرجوع إلى سطح المكتب، وإذا تم إدخال كلمة مرور خاطئة تستمر شاشة التوقف في العمل. مع أن هذا الإجراء يبدو جيداً نوعاً ما، إلا أن شاشات التوقف المحمية تعطي إحساساً مزيفاً بالأمن لأنه توجد عدة طرق لاختراق شاشة التوقف التي تعمل، تطبق هذه المهاجمات في الأنظمة Windows 3.x/9.x/ME فقط، لأن شاشات التوقف في الأنظمة Windows NT/2000/XP تستخدم إجرائيات مصادقة أكثر أمناً لنظام التشغيل. بالإضافة إلى ذلك تقدم شاشات توقف من مصادر أخرى مستويات حماية أعلى من الإصدارات الافتراضية التي يتم تسويقها مع الأنظمة Windows 3.x/9.x/ME. تتضمن أنواع المهاجمات على شاشات التوقف ما يلي:

- **إعادة الإقلاع.** أبسط طريقة هي ضغط زر إعادة التشغيل للحاسب أو إطفائه ثم تشغيله مرة ثانية، بعد إعادة إقلاع الحاسب ستتمكن من الوصول إلى جميع الملفات والتطبيقات حالما يتم تحميل النظام مرة أخرى. عندما تنتهي قم بتشغيل شاشة التوقف مرة أخرى. سيئة هذا النوع من المهاجمة هو أن المستخدم الدقيق الملاحظة قد يتساءل عن سبب عدم وجود

[1] ملف التشكيل الجانبي Profile هو ملف يتضمن مجموعة إعدادات النظام الخاصة بمستخدم معين في أنظمة Windows

الملفات والتطبيقات التي كانت تعمل حين يقوم بإدخال كلمة المرور ليعود إلى سطح المكتب، يستطيع المستخدم الذكي أن يضع أمراً لتعمل شاشة التوقف من مجلد بدء التشغيل، هذا الأمر سيقوم بتحميل وتنفيذ شاشة التوقف حالما يبدأ نظام التشغيل Windows بالعمل، إذا حصل هذا اضغط الزر Shift اليساري باستمرار أثناء تحميل النظام، يمنع هذا الإجراء تشغيل أية برامج في مجلد بدء التشغيل.

- **الملف Autorun.inf.** طريقة أفضل لاختراق شاشة توقف أثناء تنفيذها هي الاستفادة من ميزة التشغيل التلقائي للقرص المضغوط CD، عند إدخال القرص في محرك الأقراص المضغوطة يبحث نظام التشغيل عن وجود ملف اسمه Autorun.inf في الجذر الرئيسي، يعرض هذا الملف تطبيقاً يتم تشغيله تلقائياً عند إدخال القرص، حتى عندما تكون شاشة التوقف فعالة. لذلك كل ما عليك فعله هو إنشاء ملف نصي باسم Autorun.inf يحتوي سطراً واحداً هو اسم البرنامج الذي ترغب بتشغيله ثم انسخ هذا الملف على القرص المضغوط. مثلاً، إذا كان السطر الأول من الملف هو Explorer.exe، سوف يظهر برنامج مدير ملفات مستكشف النظام Windows فوق شاشة التوقف.
- **استخلاص كلمة المرور.** استخدمت الإصدارات الأقدم من نظام التشغيل Windows تشفيراً ضعيفاً جداً لتخزين محتويات كلمات المرور لشاشات التوقف. توجد أدوات برمجية عديدة تقوم باستخلاص كلمة المرور (تم ذكر البعض منها في فقرة "أدوات لاختراق النظام" من هذا الفصل). يمكنك استخدام هذه الأدوات مع الملف Autorun.inf، بحيث يمكن أن تدخل القرص المضغوط وتجعله يزودك بكلمة المرور لشاشة التوقف التي تعمل.

أنظمة التشغيل Windows NT/2000/XP

إذا كان الأمن في نظم التشغيل الأقدم Windows 3.x/9.x/ME ضعيفاً، فإن الإجراءات الأمنية في النظم Windows NT/2000/XP هي مثل Lubyanka، رئيس لجنة السلامة الحكومية في موسكو KGB ورئيس السجن السابق السيئ السمعة. مع أنه قد تثبط همتك من شيء خارجي يبدو أنه أمن غير قابل للاختراق، لكنه من الداخل يملك نقاط ضعف يمكن اختراقها. (قامت وكالة الاستخبارات المركزية في أمريكا، أثناء تنفيذ عملية سرية في الثمانينات رمزها السري CK-TAW، باعتراض مكالمات الهاتف، الفاكس، والتلكس في قناة (مركز اتصالات سري في مدينة Troitsk) ربطت Lubyanka ورئيس مجلس إدارة لجنة السلامة الحكومية KGB في مدينة Yasenevo. كانت هذه العملية تزود الوكالة بكثير من المعلومات المفيدة حتى قام الخائنان Edward Howard Lee و Aldrich Ames بفضحها. لقب اللواء السابق في KGB هذه العملية "الضربة القاضية لوكالة CIA، لقد سمعوا كل المكالمات، كلها.")

بعد أن تنتهي من رواية هذه الحكاية تخبر طلابك أنه من الضروري جداً تعلّم بعض نقاط الضعف خلال عملية المصادقة لنظم التشغيل Windows NT/2000/XP وذلك عند القيام "بعملية تسجيل الدخول التفاعلي Interactive Logon" (مصطلح عائد لشركة Microsoft يشير إلى عملية التسجيل لحاسب غير متصل بشبكة)، وبذلك يطبقون عملية TAW ضد النظام.

توقع كلمات المرور: أبسط طريقة مهاجمة يمكنك أن تستخدمها للحواسب التي تعمل على أنظمة التشغيل Windows NT/2000/XP هي توقع كلمة المرور (يمكن أن تكون محظوظاً وتصادف نظاماً حيث يكون الخيار تسجيل الدخول التلقائي Automatic Logon مفعّلاً، والذي يقوم آلياً بإدخال كلمة المرور واسم المستخدم عند بدء تشغيل النظام Windows). لكن تكوين نظام التشغيل الافتراضي هو عرض اسم حساب المستخدم للشخص الأخير الذي قام بعملية تسجيل الدخول للنظام، لذلك كل ما تحتاجه هو معرفة كلمة المرور.

من الأسهل تطبيق تقنيات توقع كلمات المرور ضد أنظمة التشغيل Windows XP، حيث قامت شركة Microsoft، بهدف جعل النظام سهل الاستخدام، بتضمين ميزة تلميح لكلمة المرور Password Hint خلال عملية تسجيل الدخول. قد يملك المستخدمون المبتدئون وغير المتخصصون تلميحاً سهل التوقع.

يملك نظام التشغيل Windows حسابين افتراضيين: حساب المدير Administrator Account وحساب الضيف Guest Account، موصفان كما يلي:

- حساب المدير Administrator Account، أو أي حساب آخر يملك نفس امتيازات المدير هو الهدف الأساسي لك (هذا الحساب مكافئ للجذر "root" في نظم تشغيل UNIX). يسمح لك حساب المدير أن تحقق الوصول إلى جميع الملفات على الحاسب، باستثناء بعض منها إذا تم استخدام نظام الملفات المشفر EFS (Encrypting File System). حسابات المدير هامة لأننا نحتاجها خلال عملية استخلاص الحسابات وكلمات المرور في أنظمة Windows NT/2000/XP.
- يتم استعمال حساب الضيف Guest Account للسماح للأشخاص بامتلاك وصولاً محدداً جداً للحاسب في حال لم يكن لديهم حساباً خاصاً. افتراضياً لا يكون حساب الضيف مفعّلاً.

عليك أن تحاول استخدام توقع كلمة المرور لكلا الحسابين، بعض كلمات المرور الشائعة التي يمكن أن تجربها هي: Administrator، Guest، أو ترك حقل كلمة المرور فارغاً.



انظر الفصل السادس لمعلومات أكثر حول توقع كلمة المرور.

تشغيل الحاسب البديل: من أكثر الطرق سهولة وفعالية هي تجاوز نظام التشغيل Windows تماماً وتشغيل الحاسب باستخدام نظام تشغيل آخر، هذا يعطيك وصولاً كاملاً للملفات المخزنة على القرص الصلب من خلال نظام تشغيل آخر.

إذا كان نظام الملفات للقرص المستهدف هو FAT أو FAT32 يمكنك استخدام قرص بدء تشغيل DOS (نظام التشغيل DOS هو نظام تشغيل الأقراص، اختصار للعبارة Disk Operating System) لتشغيل الحاسب ومن ثم الوصول إلى الملفات المخزنة على القرص :C، لكن الاحتمال الأكبر هو أن يستخدم القرص الصلب نظام الملفات NTFS، والتي لا يتعرّف عليها نظام التشغيل DOS (يزود نظام الملفات NTFS مستوىً أمنياً متقدماً للملفات وذلك بتحديد امتيازات ملكية الملفات). عليك في هذه الحالة استخدام برنامج مثل NTFSDOS والذي يسمح لنظام التشغيل DOS أن يتعرّف على القرص، أو استخدام إصدار نظام التشغيل Linux الذي يدعم نظام الملفات NTFS.

نستعرض بعض الأدوات البرمجية التي تدعم هذا النوع من المهاجمات ضمن فقرة "أدوات لاختراق النظام" من هذا الفصل.

أقراص تغيير كلمات المرور للنظام: يملك نظام التشغيل Windows XP خياراً لإنشاء قرص لتغيير كلمة المرور، لأن المستخدمون كثيراً ما ينسون كلمات المرور الخاصة بهم، تملك شركة Microsoft معالجاً لتغيير كلمة المرور Forgotten Password Wizard والذي يكتب المعلومات إلى قرص مرن، إذا نسي المستخدم كلمة المرور خلال عملية تسجيل الدخول يقوم بإدخال القرص والذي يمكّنه من تغيير كلمة المرور.

مع أنه لا يمكننا ضمان أن هدفك يملك قرصاً لتغيير كلمة المرور، يجب عليك أن تمضي بعض الوقت لتفتش في مكتبه عن قرص يمكن أن يكون عنوانه كلمة المرور، كلمة المرور للنظام Windows، أو كلمة المرور للنظام Windows XP. لا أحد يعرف، قد تكون محظوظاً.

أساليب: مصادر الاستخبارات

الجاسوس الجيد يعرف نقاط القوة والضعف لخصمه (أو على الأقل يعتمد على أحد ما من منظمته ليفعل ذلك). خصمك هو نظام التشغيل Windows، وبشكل خاص الميزات الأمنية التي لا تسمح لك باختراقه، لكن يتم اكتشاف نقاط ضعف جديدة أسبوعياً وأحياناً يومياً، ويجب أن تكون مطلعاً على الثغرات الجديدة لتتمكن من استغلالها (أو تعزيزها إذا كنت مع طرف مكافحة التجسس).

السؤال الذي قد يخطر ببالنا، لماذا يقوم مصنّعو البرمجيات بإطلاق شيفرات كثيرة الأخطاء والتي تحوي الكثير من العثرات؟ مثلاً نظام التشغيل Windows.

لقد تم تقدير أن نظام التشغيل Windows NT يتضمن 20 مليون سطراً برمجياً، Windows 2000 يتضمن 35 مليون سطراً برمجياً، أما نظام التشغيل Windows XP فيتضمن 40 مليون سطراً برمجياً، يحوي هذا الكتاب حوالي 40 سطراً في الصفحة الواحدة، لذا فإن الشيفرة المصدرية لنظام XP سوف تكون مكافئة تقريباً لكتاب واحد مؤلف من مليون صفحة أو 2,500 كتاب مثل هذا الكتاب. والآن ما رأيك أن تكون مصححاً لهذا الكم الهائل من الأعمال؟

وفقاً لمعهد هندسة البرمجيات، هناك خمسة إلى خمسة عشر خطأً في كل ألف سطر من الشيفرة، إذا طبقنا هذا العدد على نظام التشغيل Windows XP سيكون هناك ما بين 200,000 إلى 600,000 خطأ. (هنا يلعب الاقتصاد دوراً هاماً، لأنه من الأرخص إنتاج ترميمات برمجية وإصدارها لاحقاً، من قضاء أشهر طويلة لتدقيق كل سطر من الشيفرة). مع أنه لن تؤثر جميع الأخطاء على الأمن إلا أن عدداً منها بالتأكيد سيفعل. لهذا السبب تكون أخطاء الأمن شائعة جداً في نظم التشغيل والتطبيقات الضخمة والمعقدة.

فيما يلي بعض المصادر التي تمكنك من مواكبة الثغرات الجديدة التي يمكن أن تستغلها لأهداف التجسس:

- **لائحة BugTraq**. وهي لائحة بريد إلكتروني تعريفية كاشفة للأمن، تتضمن جميع العثرات ونقاط الضعف لعدة أنظمة تشغيل، يتم توجيه الانتقادات لهذه اللائحة غالباً من قبل مصنّعي البرمجيات الذين تظهر أخطائهم ضمن اللائحة بسبب تزويدها الكثير من المعلومات. لمزيد من التفاصيل اتبع الرابط www.securityfocus.com/popups/forums/bugtraq/intro.shtml.
- **لائحة NTBugTraq**. تم تطوير هذه اللائحة خصيصاً لقضايا الأمن لأنظمة التشغيل Windows NT/2000/XP، للاشتراك والوصول إلى السجلات، اتبع الرابط www.ntbugtraq.com.
- **شركة Microsoft**. للحصول على نشرة أمنية كاملة لشركة Microsoft (بالإضافة إلى معلومات حول كيفية الاشتراك)، اتبع الرابط www.microsoft.com/technet/security/current.asp.
- **فريق الاستجابة لطوارئ الحاسب CERT**. لقد كانت لائحة الاستشارات والعثرات التابعة لفريق الاستجابة لطوارئ الحاسب CERT في جامعة Carnegie Mellon القانونية الفدرالية، من أول اللوائح الخاصة بالعثرات ولكنها الآن تفوقت على لائحة BugTraq من حيث التفاصيل والانتهازية والمعلومات. اتبع الرابط www.cert.org.
- **مركز حماية البنية التحتية الوطنية الحكومية الأمريكية NIPC**. يقوم المركز بجمع وكشف المعلومات عن العثرات الجديدة، بالرغم من أن المعلومات قليلة وتفتقر إلى التفاصيل إلا أنها مفيدة كنقطة انطلاق للتعرّف على مواضيع البحث في محرك البحث Google لمعلومات أشمل. اتبع الرابط www.nipc.gov.

مهاجمة مدير حسابات الأمن: يشكل ملف مدير حسابات الأمن SAM (Security Accounts Manager) أحد الأهداف الأساسية لاختراق أمن الحاسب، قبل أن نشرح كيفية مهاجمة SAM، من المفيد فهم كيفية عمل إجراء مصادقة تسجيل الدخول، بعد أن يبدأ الحاسب بالعمل ويجتاز عملية تسلسل الإقلاع، يمر عبر الخطوات التالية:

1. ينفذ الملف Winlogon.exe كآخر خطوة من إجراء الإقلاع.
2. يتصل الملف Winlogon.exe بالملف Msgina.dll لاستعراض شاشة الترحيب في النظام Windows XP أو مربع حوار تسجيل الدخول في الأنظمة Windows NT/2000.
3. ينقل الملف Winlogon.exe حساب المستخدم وكلمة المرور لنظام سلطة الأمن المحلي الفرعي LSA (Local Security Authority)، والذي يتحقق من الملف SAM للتأكد من صحة اسم الحساب وكلمة المرور.
4. إذا كان اسم الحساب وكلمة المرور صحيحان، يعيد مدير حسابات الأمن SAM معرّف أمن المستخدم SID (Security Identifier) ومعرّفات المجموعات التي ينتمي إليها المستخدم.
5. ينشئ نظام LSA علامة للوصول مبنية على هذه المعلومات، تمنح علامة الوصول هذه الوصول للموارد المحمية بناءً على سماحيات Permissions وامتيازات الوصول Access Privileges[1] الخاصة بالمستخدم.
6. يحمّل الملف Winlogon.exe موجه أوامر النظام Windows مع علامة المستخدم.

يعتبر ملف مدير حسابات الأمن SAM من مجوهرات الأمن لنظام التشغيل Windows لأنه يتضمن جميع حسابات وكلمات المرور الخاصة بالمستخدمين. يحفظ هذا الملف ممزوجاً باستخدام تابع تجزئة باتجاه واحد one-way hash function[2] لكي لا يتم كشف معلومات كلمة المرور بشكل مباشر. يتوضع الملف SAM ضمن السار winnt\system32\config\sam للأنظمة Windows NT/2000 وضمن المسار windows\system32\config\sam لنظام Windows XP (أما في أنظمة Windows 2000 Server والتي تعمل كوحدات التحكم بالمجال ، يتم تخزين

---

[1] امتيازات الوصول Access Privileges: حق يعطى للمستخدم يمكنه من فتح وتعديل الأدلة والملفات والبرامج المتوضعة في حاسب آخر ضمن الشبكة. وامتيازات الوصول هذه يؤمنها المشرف على الشبكة أو ما يُدعى بمالك موارد الشبكة، وهي تحدد من الذي يستطيع الوصول إلى الحاسب وما الذي يستطيع فعله.

[2] تابع تجزئة باتجاه واحد one-way hash function: وهو تابع رياضي يقوم بتحويل رسالة من أي طول إلى رمز بطول ثابت، وبحيث يكون هذا الرمز مميزاً للرسالة الأصلية. ومع ذلك لا يمكن تحديد محتوى الرسالة الأصلية بوساطة تحليل الرمز. يمكن استخدام تابع تجزئة باتجاه واحد لتحديد فيما إذا كان قد تم تغيير رسالة ما أثناء نقلها عبر الشبكة، حيث يتم إرسال الرمز مع رسالة مشفرة ويقوم الحاسب المستقبل بتطبيق تابع التجزئة نفسه على الرسالة بعد فك تشفيرها. وإذا كان هناك اختلاف بين الرمزين، فذلك يدل على أنه قد تم تغيير الرسالة في الطريق.

معلومات الحساب وكلمة المرور في الدليل النشط[1] Active Directory وليس في ملف مدير حسابات الأمن SAM.

إذا تم كشف ملف SAM، فيوجد هناك الكثير من البرامج الخدمية التي تمنح الجاسوس وصولاً كاملاً للنظام، فيما يلي بعض التقنيات لمهاجمة ملف SAM:

- **حذف ملف SAM أو إعادة تسميته.** إذا قمت بإقلاع الجهاز باستخدام نظام تشغيل آخر ولديك وصول كامل قراءة وكتابة للقرص الصلب، بالتالي يمكنك حذف أو إعادة تسمية الملف. والآن لا يوجد أي حسابات في النظام بعد أن تعيد الإقلاع فبإمكانك أن تسجل الدخول على حساب المدير وتترك حقل كلمة المرور فارغاً. (دائماً عندما تغير ملف SAM فيزيائياً، سواء حذفه أو تعديله، عليك إنشاء نسخة احتياطية أولاً).
- **مهاجمة ملف SAM في الزمن الحقيقي.** إذا كان الحاسب الهدف يعمل مسبقاً فيمكنك أن تنصب وتشغّل برنامج خدمي لمهاجمة الملف SAM (تحتاج إلى امتيازات المدير) لتحاول أن تكشف حسابات الجهاز.
- **مهاجمة ملف SAM بدون اتصال.** عليك الحصول على معلومات الملف SAM من الحاسب الهدف ومن ثم تشغيل برنامج خدمي للمهاجمة من موقع آخر. عند العمل على الإصدارات الأقدم من Windows NT تستطيع أن تعيد إقلاع الحاسب باستخدام نظام تشغيل آخر وتنسخ الملف إلى قرص، أما بالنسبة لأنظمة التشغيل Windows XP/2000 والتي تملك أمناً أفضل لتحويل كلمات المرور، يجب أن تتمتع بامتيازات المدير وتنفذ برنامجاً خدمياً والذي يستخلص تحويل الملف SAM من الحاسب الهدف وثم تخزينها إلى قرص.
- **تعديل الملف SAM.** توجد مجموعة من البرامج الخدمية والتي تغير كلمات المرور للحسابات في الملف مباشرة، عليك الإقلاع من قرص البرنامج الخدمي ثم اختر الحساب الذي تريد تغييره، حساب المدير مثلاً ومن ثم حدد كلمة مرور جديدة.

من وجهة نظر الحصانة فإن التجزئة باتجاه واحد في أنظمة Windows NT ضعيفة وقابلة للتعرض إلى مهاجمات المخربين والتي قارنت كلمات المرور للحسابات المجزئة بكلمات المرور المتوقعة، واجهت شركة Microsoft هذا الضعف بتقديمها ما يسمى النظام المفتاحي Syskey (System Key) في الحزمة الخدمية الثالثة Service Pack 3 لنظام التشغيل NT 4.0 والإصدارات اللاحقة من النظامين Windows 2000/XP.

[1] الدليل النشط: خدمة دليل في نظام Microsoft Windows 2000 تؤمن إدارة مركزية للمصادقة وخدمة التطبيقات وتسجيل المستخدمين لبيئة شبكة موزعة.

يضيف النظام المفتاحي طبقة إضافية من الحماية للملف SAM بتشفيره باستخدام مفتاح طوله 128 bit، وهذا يجعل من المستحيل تقريباً اختراق ملف SAM باستخدام النظام المفتاحي. تم تفعيل النظام المفتاحي Syskey في النظام NT 4.0 يدوياً، لكنه دخل افتراضياً في الأنظمة Windows 2000/XP. (حتى فترة قريبة، لم تستطع البرامج الخدمية للمهاجمة أن تميز بين ملف SAM المشفر باستخدام النظام المفتاحي والملف العادي دون تشفير، وكانت تدور هذه البرامج مع المعالج لأيام وأسابيع محاولة اكتشاف كلمات المرور التي من المستحيل أن تكشف بسبب وجود طبقة التشفير الإضافية).

بالرغم من أن النظام المفتاحي يحمي من هؤلاء الذين يحاولون كشف ملف SAM بشكل مباشر، لكنه لا يزود الحماية من استخلاص كلمات المرور المجزأة من الذاكرة مباشرة (إذا كنت تملك امتيازات المدير) أو من حركة المرور المصادقة عبر الشبكات. يتم استخدام تحويل كلمات المرور لمدير الشبكة المحلية الأقدم والأقل أماناً للمصادقة، في الشبكات التي تتضمن مزيجاً من أنظمة التشغيل Windows 9x/ME وأنظمة التشغيل Windows NT/2000/XP. يمكن حفظ التحويل المخزن في الذاكرة أو المستخلص من شبكة ومن ثم استخدامه في برنامج لتغيير كلمة المرور بكل سهولة.



عند محاولتك تعديل الملف SAM، في نظام Windows XP Professional الذي يستخدم نظام الملفات Encrypting File System) EFS)، عن طريق حذفه أو تعديل كلمة مرور لحساب ما محمي بنظام الملفات EFS فإنك تخاطر بأن تفقد الوصول لأي بيانات مشفرة. لكن هذا لا يطبق على الملفات والمجلدات المحمية بنظام الملفات EFS في النظام Windows 2000، حيث يستطيع أي مستخدم يملك امتيازات المدير أن يحقق الوصول إلى الملفات المشفرة بقيامه ببساطة تغيير كلمة المرور للحساب نفسه. لا يدعم نظام التشغيل Windows XP Home نظام الملفات EFS.

الامتيازات المتصاعدة: دعنا نفترض أنك تستطيع تسجيل الدخول إلى حاسب باستخدام حساب الضيف غير المؤمن، في الحقيقة ليس هناك الكثير مما يمكنك فعله لأن سماحيات نظام الملفات NTFS تبقيك بعيداً عن ملفات المستخدمين الآخرين، وتحتاج إلى امتيازات المدير لتتمكن من استخدام أية برامج خدمية لكلمات المرور للملف SAM.

على أية حال، بما أنك أصبحت داخل النظام مع الحساب الذي لا يتمتع بأي امتيازات، يمكنك أن تنفذ مهاجمة ذات الامتيازات المتصاعدة. تتضمن هذه المهاجمة الاستفادة من شيء يسمى تدفق النظام المعروف الذي يسمح لك أن تنفذ عملاً ما بحيث يعتقد نظام التشغيل بأنك تملك الامتيازات لكنك في الواقع لا تملكها. تستطيع بوساطة الامتيازات المتصاعدة أن تضيف، تحذف، أو تعدل بيانات النظام، إنشاء أو حذف حسابات المستخدمين، أو إضافة حسابات إلى مجموعة المدراء.

فعلى سبيل المثال، يتضمن استغلال شائع في بيئة نظام التشغيل Windows 2000 خدمة تسمى NetDDE، حيث تم اكتشاف أنه عندما تعمل هذه الخدمة تستطيع تنفيذ أوامر باستخدام امتيازات النظام. (تُمنح هذه الامتيازات للعمليات التي تعمل على مستوى نظام التشغيل، تخيلها مثل امتيازات المدير الخارق). مثلاً، يؤدي إدخال الأمر التالي ضمن سطر الأوامر إلى تمكين أي مستخدم كان قد قام بعملية تسجيل دخول تفاعلية إلى النظام، بغض النظر عن امتيازاته، من تنفيذ البرنامج cmd.exe والوصول إلى جميع ملفات القرص الصلب:

```
C:\>netddemsg –s Chat$ cmd.exe
```

تم نشر مهاجمات جديدة للامتيازات المتصاعدة، تحاول شركة Microsoft أن تصدر ترميمات أمنية لمواجهة هذه المشكلة. (يمكن أن تكون فترة الاستجابة للمشكلة سريعة جداً أو بطيئة جداً، مثلاً، تم الاعتراف وترميم المهاجمة التصاعدية، والتي استخدمت الحدث WM_TIMER والذي انتشر بشكل واسع في شهر آب من عام 2002 وسمحت لأي مستخدم قام بعملية تسجيل الدخول بالتحكم ضمنياً بالنظام بكامله، في شهر كانون الأول من نفس العام). غالباً لا يدرك المستخدمون إصدارات الترميم هذه وحتى لو كانوا يدركونها فلن يقوموا بتنصيبها، يمكن أن ينفعك هذا الأمر.

أدوات لاختراق النظام

تخبر طلابك أنه من غير المجدي فتح دمية الماتروشكا يدوياً، طالما هناك أدوات مجانية تجارية كثيرة تسّهل عليك هذه المهمة كثيراً. ثم توزع لائحة تحتوي بعض البرامج الخدمية الشائعة لاختراق أمن النظام، وتشرح كل منها باختصار.

أدوات لمهاجمة كلمات المرور الخاصة بنظام الدخل/الخرج الأساسي BIOS

يتوفر عدد من البرامج الخدمية التي تكشف كلمات المرور للنظام BIOS، لكن شرط استخدام هذه البرامج هو إقلاع الحاسب بنجاح وتنفيذها أثناء عمله. إذا واجهت مشكلة إدخال كلمة

مرور للنظام BIOS عند إقلاع الحاسب عليك أن تستخدم طريقة أخرى للوصول إلى القرص الصلب، كما هو مشروح في فقرة "استغلال نقاط الضعف" من هذا الفصل.

CMOSPWD أحد البرامج الخدمية الأكثر شهرة واستخداماً للنظام BIOS، وهو عبارة عن أداة سطر الأوامر مبرمجة من قبل Christophe Grenier. يستخلص هذا البرنامج كلمات المرور من الإصدارات التالية للنظام BIOS:

Acer/IBM	**IBM Thinkpad boot password**
AMI BIOS	**Packard Bell Supervisor/User**
AMI WinBIOS (12/15/93)	**Phoenix 1.00.09.AC0 (1994)**
AMI WinBIOS 2.5	**Phoenix 1.04**
Award 4.5x	**Phoenix 1.10 A03/Dell GXi**
Award Medallion 6	**Phoenix 4 release 6 (User)**
Compaq	**Phoenix 4.05 rev 1.02.943**
Compaq (1992)	**Phoenix 4.06 rev 1.13.1107**
Gateway Solo — Phoenix 4.0 r6	**Phoenix A08, 1993**
IBM (PS/2, Activa)	**Toshiba**
IBM 300 GL	**Zenith AMI**

في حال لم يتمكن هذا البرنامج من استخلاص كلمة المرور، فهو يملك خياراً للتخلص منها نهائياً. البرنامج Cmospwd هو برنامج سهل الاستخدام، فعال، وموثق بشكل جيد، يحتوي الملف المساعد Readme كثيراً من المعلومات المرتبطة بالمهاجمات على النظام BIOS. لتحميل الأداة، اتبع الرابط www.cgsecurity.org/index.html?cmospwd.html.

أدوات أخرى تتوفر أدوات برمجية أخرى تطبق على إصدارات محددة من نظام BIOS، ومن الجدير امتلاك مجموعة من هذه الأدوات لأن أحدها سوف تقوم بعمل بشكل أفضل من الأخرى. نقطة انطلاق جيدة لتبدأ بتجميع صندوق الأدوات الخاص بك لاختراق الأنظمة هي "مخربو كلمات المرور لأنظمة BIOS" والمعروضة على الرابط:

www.packetstormsecurity.org/crackers/bios.

أدوات لمهاجمة أنظمة التشغيل Windows 3.X/9.X/ME

بما نه لا يوجد أمن مصادقة عند تسجيل الدخول في عائلة أنظمة التشغيل Windows 3.x/9.x/ME، فإنه تقع المهاجمات الحقيقية على مستوى النظام (غير الشبكي) عند تشغيل شاشة توقف. (يتم شرح أدوات المهاجمة الأخرى التي تقوم بكشف تشفير التطبيق وأمن الشبكات في جميع إصدارات أنظمة Windows في الفصلين السادس والعاشر). تتضمن أدوات مهاجمة شاشات التوقف ما يلي:

- **Ratware Win9x Screen Saver Buster**. عندما تنسخ هذه الأداة على قرص مضغوط وتستخدمها مع ملف التشغيل التلقائي Autorun.inf، يقوم البرنامج آلياً بإطفاء شاشة التوقف العاملة. يمكنك تحميل هذه الأداة من الرابط التالي:

http://packetstormsecurity.org/Win/RWSaverBust.zip.

- **Scrsavpw**. يمكنك تحميل هذه الأداة التي تجتاز كلمة المرور، والمبرمجة من قبل Matthias Bockelkamp، من الرابط www.geocities.com/mbockelkamp/.

أدوات لمهاجمة أنظمة التشغيل Windows NT/2000/XP

يتوفر عدد من الأدوات التجارية المجانية يتم استخدامها لأهداف غير معقدة، وذلك بسبب شيوع أنظمة Windows في بيئات العمل المشترك وحاجة المدراء لإنجاز تدوين أمني واستعادة البيانات من الأنظمة المغلقة. نستعرض فيما يلي بعض الأدوات الشائعة بين الجواسيس والمدراء أيضاً، الخاصة ببيئات أنظمة Windows NT/2000/XP:

LC (L0PHTCRACK) يعتبر البرنامج الخدمي L0phtCrack أشهر أداة لتحطيم كلمات المرور في الأنظمة Windows NT/2000/XP، سمي بهذا الاسم نسبة إلى اسم مجموعة القرصنة للصناعات الثقيلة L0pht قبل أن يصبحوا جزءاً من الشركة @Stake، المختصة بالاستشارات الأمنية). تم تغيير اسم الإصدار الرابع من هذه الأداة إلى الاسم LC4 لإبعادها عن أصولها الحرة التابعة للقراصنة.

بدأت الأداة LC، التي برمجها أصلاً Peiter Zatko (اسمه المستعار Mudge)، بالظهور عام 1997 كبرنامج خدمي يتميز بالقوة العمياء[1] لتحطيم كلمات المرور. لقد تطورت هذه الأداة منذ ذلك الحين إلى أداة برمجية معقدة ذات واجهة سهلة الاستخدام (الشكل 4-2)، فيما يلي نعرض عدداً

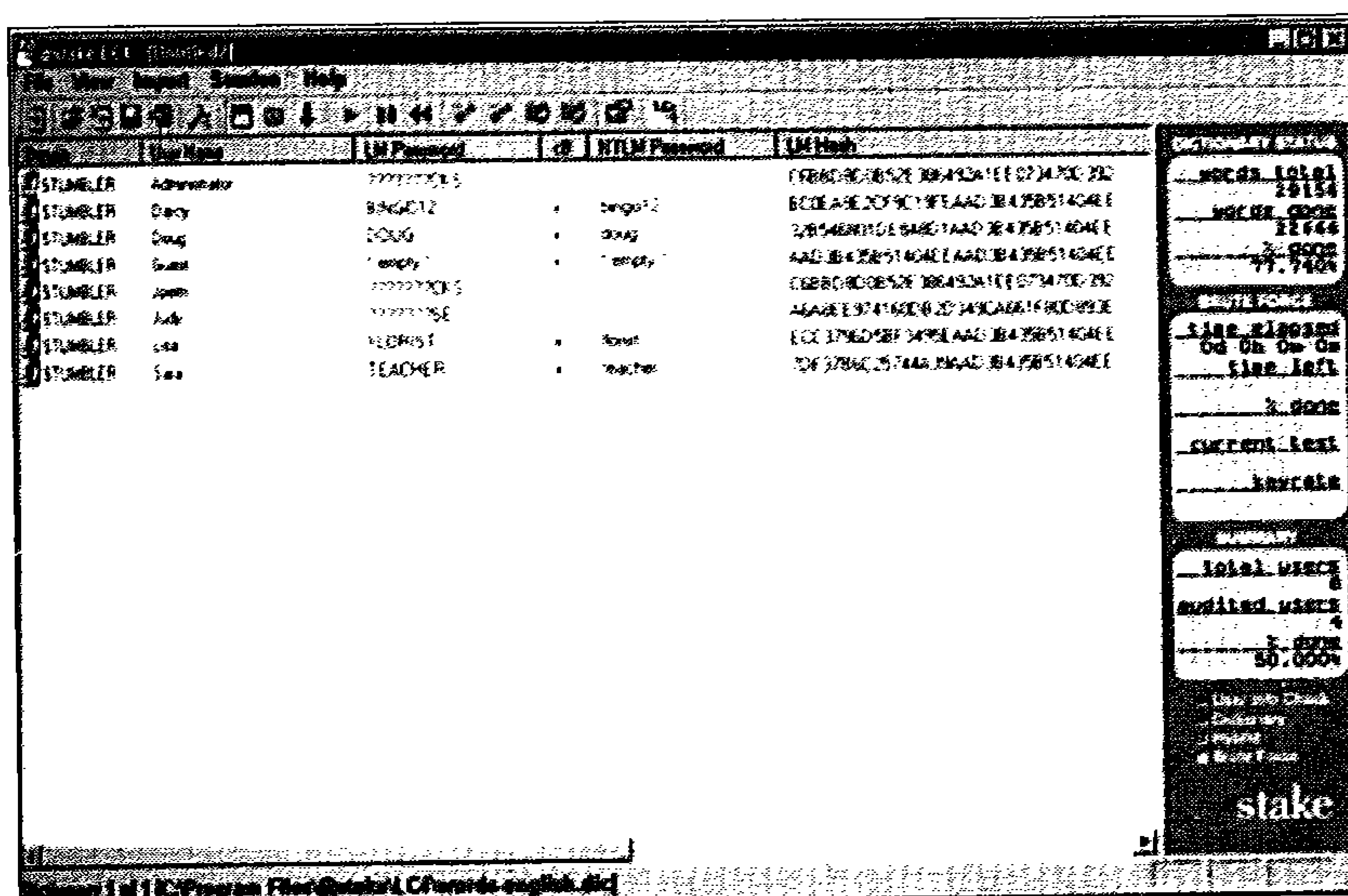
[1] طريقة القوة العمياء Brute-force method: طريقة من طرق حل المشكلات باستخدام الحاسب. تعتمد هذه الطريقة، كما يشير اسمها، على القوة الهائلة للحاسب وبدون الاعتماد على التقنيات البرمجية الذكية، أي أنها تستخدم تقنيات تستفيد من الخصائص الهائلة للحاسب مثل سرعة أدائه للعمليات وكذلك الحيز التخزيني الكبير. في مقابل ذلك يمكن استخدام بعض الطرق (الخوارزميات) الذكية لإنجاز نفس العمل، وباستخدام موارد أقل من موارد الحاسب. لا يعتمد المبرمجون عادة على هذه الطريقة إلا إذا كانت الخيار الأمثل أو الحل الوحيد.

من الطرق لتوزيع مهاجمة القوة العمياء بين مجموعة من الحواسب، والحصول على تحويل كلمات المرور:

- **الاستيراد من الآلة المحلية.** يسترجع البرنامج LC جميع الحسابات وتحويلات كلمات المرور من الحاسب المحلي، تحتاج إلى امتيازات المدير للقيام بهذا.
- **الاستيراد من التسجيل البعيد.** إذا كان خيار الوصول إلى التسجيل البعيد مفعّلاً في الحاسب، فبإمكانك استيراد التحويلات من الأنظمة حيث لا يتم استخدام النظام المفتاحي Syskey.
- **ملفات مدير حسابات الأمن SAM.** يقرأ برنامج LC التحويلات المنسوخة من الأنظمة التي لا تملك خيار النظام المفتاحي Syskey مفعلاً، من ملف SAM مباشرة.
- **الاكتشاف.** يستطيع البرنامج الاستيلاء على تحويلات كلمات المرور من التسلسل اعتراض/ استجابة عندما يصادق حاسب حاسباً آخر من خلال شبكة Ethernet.
- **Pwdump.** يستورد البرنامج خرج أداة تجميع تحويلات كلمات المرور Pwdump، يرد شرح هذه الأداة لاحقاً.
- **استيراد ملفات من الإصدارات السابقة للبرنامج LC.** يدعم الإصدار الحالي من البرنامج الإصدارات السابقة له، والتي استخدمت تنسيق مختلف للملفات لتخزين معلومات الحساب وكلمة المرور.

بعد تحميل تحويلات كلمات المرور إلى البرنامج، ينفذ البرنامج مهاجمة القاموس، مهاجمة قاموسية هجينة تقوم بالإضافة، أو الاستبدال للأحرف الشائعة الاستخدام في الكلمات، أو مهاجمة القوة العمياء (بلغ معدل مهاجمة القوة العمياء حوالي 2.8 مليون كلمة مرور في الثانية باستخدام معالج Mobile Pentium III سرعته 1000-MHz).

البرنامج LC ليس رخيصاً سعره 350 دولاراً أمريكياً، لكنه من الأدوات البارزة لاختراق أمن النظام (أو شرعياً تدوين كلمات المرور). لمزيد من المعلومات ولتحميل نسخة تجريبية من البرنامج، اتبع الرابط www.atstake.com.



الشكل (4-2) برنامج (L0phtCrack) LC4 وهو في حالة التنفيذ ضد مجموعة من تحويلات كلمات المرور. تم كشف بعض الحسابات عن طريق مهاجمة القاموس والبعض الآخر يتعرض لمهاجمة القوة العمياء.

أساليب: حلم الحصول على GINA

GINA هي آلية الترخيص والتعريف الرسومية لأنظمة Windows NT/2000/XP، تتوضع هذه الآلية بين المستخدم وخدمة مصادقة تسجيل الدخول لنظام التشغيل وتعرض مربع حوار تسجيل الدخول.

إحدى طرق مهاجمة نظام التشغيل هي استخدام تطبيق مزيف لعملية تسجيل الدخول، سيعتقد المستخدم العادي أنه يقوم بعملية تسجيل الدخول الاعتيادية، لكن في الحقيقة سيقوم تطبيق حصان طروادة[1] (مفعّل من قبل الجاسوس) بتسجيل اسم الحساب وكلمة المرور قبل أن يتم دخول المستخدم إلى النظام. اعتقدت شركة Microsoft أنه إذا تم إدخال تركيب المفاتيح Ctrl+Alt+Del إلى عملية تسجيل الدخول، فإن ذلك سيحبط تطبيقات طروادة عند تسجيل الدخول، لأن تسلسل المفاتيح هذا يستخدم لإعادة إقلاع البرمجيات والتجهيزات الصلبة.

لكن، شركة Microsoft لم تأخذ حسابها من المبرمجين الأذكياء مثل Arne Vidstrom، والذي قام ببرمجة ما يسمى GINA المزيفة. تعترض GINA المزيفة الاتصالات بين تسجيل الدخول لنظام Windows و GINA العادية، تستولي على المجال، اسم المستخدم، وكلمة المرور من جميع

[1] حصان طروادة: برنامج مدمر متنكر بشكل لعبة أو خدمة أو تطبيق، ويؤدي إلى تلف نظام الحاسب عند تنفيذه.

عمليات التسجيل الناجحة، ثم تكتب المعلومات إلى ملف نصي. لسوء الحظ، هذا ما كانت تحاول تجنبه شركة Microsoft في البداية. تعمل GINA المزيفة بنسخ ملف DLL صغير إلى المجلد system32\ وتعدّل تسجيل النظام لكي يشير مفتاح GinaDLL إلى الملف fakegina.dll (Gina المزيفة). عندما يقوم المستخدم بتسجيل الدخول إلى نظام Windows NT4.0 أو النظام Windows 2000، يتم الاستيلاء على اسم الحساب وكلمة المرور ويتم حفظهما في ملف نصي اسمه passlist.txt. يتوفر تطبيق FakeGINA على الرابط www.ntsecurity.nu/toolbox/fakegina/.

مستكشف أمن الشبكات المتطور: وهو برنامج تجاري لتحطيم كلمات المرور والذي يشن مهاجمات القاموس، مهاجمات المحارف المقنعة (أي إذا كانت محارف محددة من كلمة المرور معروفة، سوف تدخلها، والمحارف المجهولة فقط يتم توقعها)، ومهاجمات القوة العمياء. يمكن استخلاص تحويلات كلمات المرور من الذاكرة، تسجيل النظام، أو يتم استيرادها عن طريق أدوات استخلاص كلمات المرور مثل أداة Pwdump. بلغ معدل مهاجمة القوة العمياء، بأداء بارع، حوالي 2 مليون كلمة مرور في الثانية باستخدام معالج Mobile Pentium III سرعته 1000-MHz. تبلغ قيمة شراء برنامج مستكشف أمن الشبكات المتطور 49 دولار أمريكي مقابـــل الحصـــول على ترخيـــص لمستخـــدم واحد، وتتوفـــر نسخة تجريبية على الرابط www.elcomsoft.com/antexp.html.

أداة PWDUMP: وهي أداة سطر الأوامر لتفريغ تحويلات كلمات المرور في الأنظمة Windows NT/2000/XP. صممت هذه الخدمة، المبرمجة أصلاً من قبل Jeremy Allison، لاستخلاص اسم الحساب وكلمة المرور من الملف SAM باستخدام تقنية تعرف باسم حقنة DLL. دون أن ندخل إلى التفاصيل التقنية، تجبر خدمة Pwdump عملية خدمة سلطة الأمن المحلية بتحميل ملف DLL وتنفيذ الشيفرة الموجودة في فراغ عنوان العملية من أجل الوصول إلى تحويلات كلمات المرور. عندما قدمت شركة Microsoft النظام المفتاحي Syskey كطريقة لحماية ملف SAM بشكل أفضل، فقد تغلبت على مهاجمات Pwdump، رداً على هذا طوّر المبرمج Todd Sabin برنامج Pwdump2، والذي يقوم باستخلاص تحويلات كلمة المرور حتى لو كان النظام المفتاحي مفعّلاً، كما طوّر المبرمجان Phil Staubs و Erik Hjelmstad الإصدار الثالث من البرنامج Pwdump3 المبني على الإصدار الذي قبلهPwdump2 والذي يستخلص تحويلات كلمة المرور من الحواسب البعيدة عبر الشبكات. بعد أن يستخلص برنامج Pwdump التحويلات المطلوبة يتم استخدامها كدخل لبرامج تحطيم كلمة المرور مثل برنامج LC أو مستكشف أمن الشبكات المتطور. يجب أن تتمتع بامتيازات المدير لتستطيع استخدام أي إصدار من البرنامج Pwdump لاستخلاص تحويلات كلمة المرور.

جميع إصدارات برنامج Pwdump مجانية ويمكنك تحميلها من الروابط:

- Pwdump2 (http://razor.bindview.com/tools/index.shtml)
- Pwdump3 (www.polivec.com/pwdump3.html)

أداة ERD COMMANDER: وهي أداة متعددة الأغراض تستخدم في أنظمة Windows NT/2000/XP والتي تعمل كقرص مضغوط للقراءة فقط قابل للإقلاع. تم تصميم هذا المنتج لمساعدة المدراء في إصلاح وتشخيص الأنظمة التالفة، لكنه يتضمن بعض الميزات المساعدة للجاسوس أيضاً، من بينها إمكانية تغيير كلمات المرور، تحرير تسجيل النظام، نسخ، نقل، حذف الملفات، وتنفيذ أوامر النظام. إن منتج ERD Commander مناسب للمستخدمين الذين لا يتمتعون بمهارات تقنية عالية، لأنه يملك واجهة سهلة الاستخدام جداً والتي تبدو وكأنك تستخدم سطح المكتب للنظام Windows. تبلغ قيمة الإصدار الحالي من البرنامج ERD Commander 2002، 399 دولار أمريكي، ويمكنك الحصول على مزيد من المعلومات من الموقع، www.winternals.com.

أداة CIA COMMANDER: وهو برنامج خدمي ألماني مطور من قبل Datapol والذي يصل إلى المستوى المتوقع لاسمه الجاسوسي. تقوم الخدمة باستبدال كلمات المرور للحسابات في ملف SAM، تحفظ كلمات المرور القديمة لاستبدالها ليتم استرجاعها لاحقاً، تعدّل آلية الترخيص والتعريف الرسومية GINA لتجاوز أنظمة المصادقة المتناوبة مثل قارئات البطاقات الذكية، وتندمج مع مدير الملفات الشجرية لتتمكن من نسخ وحذف الملفات بسهولة على القرص المطلوب. برنامج CIA Commander ذو حجم صغير بحيث يمكن أن ينسخ على قرص مرن ويملك واجهة سهلة الاستخدام، مسعّر بقيمة 249 دولاراً أمريكياً مع توفر نسخة تجريبية على الموقع، www.ciacommander.com.

أساليب: تنظيم القاعدة ضد مجلة Wall Street

أعلنت مجلة Wall Street في شهر كانون الثاني (يناير) عام 2002، عن قيامها بسرقة ملفات من حواسب تعمل على أنظمة Windows 2000 من رؤساء تنظيم القاعدة في كابول. كانت الحواسب تستخدم نظام الملفات المشفر EFS (Encrypting File System)، لكن إصدارات أنظمة Windows كانت أقدم وذات تشفير ضعيف نسبياً تستخدم مفتاح طوله 40 بت، مقابل إصدارات نظام تشغيل أحدث ذات تشفير أقوى بكثير في أمريكا والذي استخدم مفتاحاً بطول 128 بت، وفقاً للتقارير، تم الحصول على كلمات المرور خلال خمسة أيام باستخدام تجمع من الحواسب.

يملك نظام الملفات المشفر EFS مجموعة من نقاط الضعف الخطيرة ضمن نظام التشغيل Windows 2000. افتراضياً يملك المدير حق الوصول إلى جميع الملفات والمجلدات المشفرة، بغض النظر عن صاحبها. إذا كشف جاسوس بنجاح كلمة المرور الخاصة بمدير النظام، فهو الرابح. بالإضافة إلى ذلك، في حال تم تغيير كلمة المرور لمستخدم مرتبط بالملفات المشفرة باستخدام برنامج خدمي مثل Chntpw، فإنه يمكن الوصول إلى هذه الملفات أيضاً.

من الغريب في الأمر أن مجلة Wall Street لم تستخدم هذه المهاجمات، لكن بما أنه لم يتم كشف تفاصيل العملية، فلا توجد أدلة لإدانتها. أحد الاحتمالات الممكنة هي الاهتمام باكتشاف كلمة المرور بالإضافة إلى الرغبة بالوصول إلى الملفات المحمية باستخدام نظام الملفات المشفر EFS.

ماسحات السجل: تتضمن أنظمة التشغيل Windows NT/2000/XP القدرة على تسجيل الأحداث (بالرغم من عدم تفعيل تسجيل الأحداث الأمني افتراضياً). لا تترك المهاجمات التي لا تحتاج إلى اتصال، أية آثار في السجلات ورائها. حيث تقوم باستخدام نظام تشغيل آخر لإقلاع النظام ومن ثم تتعامل مع الملفات المطلوبة على القرص الهدف، بينما قد تترك المهاجمات التي تستخدمها بينما يكون الحاسب في حالة عمل بعض العلامات لنشاطاتك. إذا كنت حذراً فقد ترغب بالتخلص من أي دليل لأفعالك.

Arne Vidstrom خبير أمني سويدي ومطوّر مثمر لأدوات أمنية مجانية لنظام التشغيل Windows. يتضمن موقعه الإلكتروني على الإنترنت، www.ntsecurity.nu، عدداً من الأدوات المفيدة للتجسس (أو الإدارة الشرعية للنظام). يقدّم Vidstrom أداتين لمسح السجلات:

- **الأداة ClearLogs**. وهي أداة سطر الأوامر تقوم بمسح الأمن، النظام، أو سجلات أحداث التطبيق.
- **الأداة WinZapper**. تسمح لك هذه الأداة باختيار الأحداث يدوياً لمسحها ضمن سجل النظام بالنسبة لأنظمة التشغيل Windows NT 4.0 وWindows 2000.

لكن السجل الفارغ قد يثير الشكوك لدى مدير النظام أو مستخدم مدرك للأمن. طريقة أخرى هي القيام بإتلاف السجل عمداً في محاولة لجعل المستخدم يعتقد أن لديه مشاكل في نظام الملفات مثل وجود وسائط تالفة. لكن أفضل الحلول هو حذف السجلات الفردية انتقائياً لمسح آثارك.

أدوات بديلة لنظم التشغيل: يمكن استخدام أنظمة تشغيل أخرى مثل DOS، أو Linux لإقلاع نظام يستخدم الأنظمة Windows NT/2000/XP، تستطيع إنشاء قرص إقلاع يحوي برامج

تشغيل أو خدمات ملائمة تدعم نظام الملفات NTFS ومهاجمة النظام، عن طريق استعراض، تعديل، أو نسخ الملفات على القرص الصلب. (يمكن تهيئة محركات أو أقسام محرك القرص في الأنظمة Windows NT/2000/XP، إلى نظام الملفات FAT، FAT32، أو NTFS. إذا تمت تهيئة محرك القرص الهدف إلى نظام الملفات FAT أو FAT32 يمكنك أن تحقق الوصول إلى القرص الصلب باستخدام قرص إقلاع للنظام DOS).

إلا أن الحواسب الجديدة التي تعمل على الأنظمة Windows 2000/XP تكون مهيأة إلى نظام الملفات NTFS ولا يمكن الوصول إليها باستخدام قرص DOS دون خدمة خاصة تدعى NTFSDOS. بعد تشغيل خدمة NTFSDOS، يمكنك أن تركيب الأقراص من نظام التشغيل DOS. يوجد إصداران من الخدمة NTFSDOS: إصدار مجاني يزود وصول للقراءة فقط وإصدار تجاري يزودك بإمكانية القراءة والكتابة. يمكنك أن تستفيد من إصدار القراءة فقط للتسلل خلال القرص الصلب واستعراض ونسخ الملفات. (إذا كانت الملفات أو المجلدات محمية بنظام الملفات المشفر EFS، لا يمكنك قراءتها بكلا الإصدارين).

- تتوفر النسخة المجانية للبرنامج الخدمي NTFSDOS على الموقع www.sysinternals.com.
- أمـــا النسخـــة التجاريـــة المسعّـــرة بقيمـــة 299 دولار أمريكي فتتوفـــر على الموقـــع، www.winternals.com.

يوجد أيضاً برنامجان خدميان للنظام Linux تستطيع استخدامهما لمهاجمة أنظمة التشغيل Windows NT/2000/XP:

- **برنـــامج Chntpw (Change NT password)**. وهي خدمـــة سطـــر الأوامـــر، برمجهـــا Peter Nordahl-Hagen، والتي تمكنك من تغيير كلمة المرور لحساب مستخدم ما ضمن ملف SAM. جعل Hagen هذا البرنامج سهل الاستخدام للأشخاص الذين لا يستخدمون نظام التشغيل Linux بتضمين صورة لقرص بدء تشغيل خاص بالنظام Linux مع دعم لنظام الملفات NTFS والذي يمكن أن ينسخ بسهولة إلى قرص مرن أو إلى قرص مضغوط، ما عليك فعله هو إقلاع الحاسب باستخدام الصورة المخزنة على القرص وتشغيل البرنامج. برنامج Chntpw مجاني ويمكنك تحميله من الرابط http://home.eunet.no/~pnordahl/ntpasswd/.
- **برنامج John the Ripper**. وهو برنامج شهير لتحطيم كلمات المرور ويعمل على أنظمة مختلفة ويتميز بمجموعة غنية من الخصائص، ويزود الشيفرة المصدر للنظام Linux، ويمكنك أن تترجم ترميم برمجي تابع لطرف ثالث والذي سيحطم كلمات المرور للملف SAM. يتوفر برنامج John على الرابط www.openwall.com/john/.

أساليب: شاشة توقف أم الندم؟

توجد طريقة أخرى لمهاجمة النظام، إذا كان لديك وصول قراءة/كتابة إلى محرك القرص الصلب الهدف، وهي الاستفادة من الملف Logon.scr. عند ظهور مربع حوار تسجيل الدخول في أنظمة التشغيل Windows NT/2000/XP و في حال لم يتم استخدام لوحة المفاتيح أو الضغط على الفأرة لمدة محددة يتم تنفيذ الملف Logon.scr، ليستعرض شاشة التوقف الافتراضية.

ما عليك فعله هو إقلاع الحاسب باستخدام نظام تشغيل آخر ومن ثم إعادة تسمية الملف Logon.scr الواقع في المسار \winnt\system32\ (للنظامين Windows NT/2000)، والمسار \windows\system32\ (لنظام Windows XP). ثم انسخ الملف Cmd.exe وأعد تسمية ملف Logon.scr باسمه.

أعد تشغيل الحاسب باستخدام نظام التشغيل Windows، عند ظهور مربع حوار تسجيل الدخول انتظر حتى وقت ظهور شاشة التوقف، لكن بدلاً من تنفيذ شاشة التوقف يتم تنفيذ موجه الأوامر Cmd.exe ليعمل كعملية ضمن النظام. في هده الحالة يمكنك أن تفعل ما تشاء بالنظام من خلال سطر الأوامر، بما فيها إنشاء حساب جديد لك ذو امتيازات المدير.

الإجراءات المضادة

يوجد عدد من الإجراءات المضادة التي يمكنك استخدامها لإبعاد عناصر KGB السابقين الماكرين والجواسيس الآخرين عن اختراق أمن نظامك. ربما الإجراء المضاد الأكثر أهمية هو ضمان تقوية أمنك الفيزيائي كما ناقشنا ذلك في الفصل الثالث، كما أن منع الأشرار من الوصول الفيزيائي إلى حاسبك، جزء مهم من المعركة. وإذا كان من الصعب إبعادهم، لا تزال هناك بعض التقنيات التي يمكنك استخدامها لجعل الأمر أصعب ما يمكن عليهم لكشف بياناتك.

الإعدادات الأمنية

يوجد عدد من الإعدادات الأمنية الخاصة بنظام BIOS ونظام التشغيل تستطيع استخدامها لتقليل فرص أحد ما للحصول على البيانات الهامة من حاسبك. لكن قبل أن تغير إعداداتك بغض النظر عن إصدار نظام التشغيل الذي تستخدمه، تأكد دائماً من تنصيب الحزمة الخدمية الأخيرة لنظام التشغيل بالإضافة إلى الإصلاحات الشهيرة المرتبطة بالأمن. كما أن الجاسوس الحاسبي الجيد سيكون مطلعاً على تسلسل الأحداث المتعلقة بأي نقاط ضعف يمكنه أن يستغلها لتدمير نظامك. إن امتلاك الترميمات البرمجية الحديثة يقلل فرص نجاح المهاجمات المحلية والبعيدة.

تقدّم شركة Microsoft تنوعاً كبيراً من الأدوات ومصادر المعلومات للمحافظة على منتجاتها محمية من نقاط الضعف المعروفة، وتتضمن ما يلي:

- **النشرات الأمنية الخاصة بشركة Microsoft**: تطلق الشركة نشرات أمنية، عندما تكتشف نقاط الضعف وتطلق الإصلاحات الخاصة بها. تتوفر هذه النشرات وموارد أخرى من موقع الشركة على الرابط التالي www.microsoft.com/technet/security. كما يمكنك الاشتراك بخدمة الإشعار الأمني الخاص بالشركة، ما عليك فعله هو إرسال رسالة فارغة إلى العنوان التالي، securbas@microsoft.com ويتم تسجيلك تلقائياً إلى هذه الخدمة.
- **تطوير النظام Windows تلقائياً**: يوجد خيار، في النظامين Windows 2000/XP، يقوم بتحميل وتطوير أي إصدار برمجي أمني جديد تلقائياً. عندما تقوم بتفعيل هذا الخيار، يتصّل حاسبك دورياً بموقع Microsoft عن طريق الإنترنت، يبحث عن أي إصدارات ترميم برمجية جديدة، يحملها وينصبها على الحاسب. (في الماضي، كان هناك تأخير يصل إلى أيام وحتى أسابيع بين وقت إصدار النشرة الأمنية ووقت ظهورها في تطوير النظام Windows. لذلك إذا كنت مهتماً بأمنك، فلا تعتمد على تطوير النظام من شركة Microsoft فقط، لتبقى مطّلعاً على كل جديد).
- **مدقّق الإصلاحات الحديثة لأمن الشبكات من شركة Microsoft (Hfnetchl.exe)**: وهي خدمة تعمل كسطر الأوامر تدقّق في حال عدم وجود ترميمات برمجية أمنية لديك (تم دمج وظائف سطر الأوامر هذا، في شهر كانون الأول من عام 2002، مع أداة الاستشارة الأمنية الأساسية لشركة Microsoft (Microsoft's Baseline Security Advisor tool)). يمكنك تحميل هذه الخدمة والحصول على تعليمات استخدامها من الرابط http://support.microsoft.com/default.aspx?scid=KB;en-us;q303215.

بعد أن تأكدت أن نظام التشغيل وأية تطبيقات ممكن أن تعاني من بعض الثغرات لديك في حالة تطوير مستمر، عليك الآن استخدام الإعدادات الأمنية التالية.

نظام الدخل/الخرج الأساسي BIOS

بالرغم من وجود العديد من طرق اختراق أمن النظام BIOS، إذا كنت قلقاً حول التجسس عليك أن تستخدم كلمات المرور الخاصة بالنظام BIOS. سوف تحمي كلمات المرور هذه نظامك من المتسللين العرضيين أو المتطفلين المبتدئين، وتصعّب مهمة الخبراء قليلاً. عليك تعيين كلمات مرور للإقلاع ولتغيير إعدادات برنامج الإعداد BIOS.

أما الإجراء الأمني الآخر الذي يمكنك استخدامه فهو منع الحاسب من الإقلاع من محرك القرص المرن :A، هذا الإجراء سوف يمنع الجاسوس من الإقلاع مستخدماً نظام تشغيل آخر ومن ثم الوصول إلى القرص الصلب. تملك أنظمة الإعداد الحديثة مجموعة من الخيارات لتسلسل الإقلاع والتي تمكّن النظام من الإقلاع من محرك الأقراص المضغوطة ومن أجهزة USB، تأكد من إلغاء تفعيل هذه الأجهزة من الإقلاع. في حالة حدوث عطل في محرك القرص الصلب وتحتاج لاستخدام قرص إنقاذ (Rescue Disk)، عليك أن تدخل إلى برنامج الإعداد BIOS أولاً، ومن ثم تغيير تسلسل الإقلاع بحيث يتم التعرف على القرص المرن.

Windows 3.X/9.X/ME

إذا كنت من مستخدمي أحد أنظمة التشغيل Windows 3.x/9/x/ME، لا يوجد، في الحقيقة، الكثير لتفعله لتعزيز أمن النظام. (يمكنك على الأقل أن تمنع اختراق القرص المضغوط لشاشة التوقف، وذلك عن طريق عرض خصائص جهاز الكمبيوتر ومن ثم إلغاء تفعيل إعداد الإعلام بالإدخال التلقائي (Auto Insert Notification) لمحرك الأقراص المضغوطة من بوابة إدارة الأجهزة .((Device Manager)

إذا كان الجاسوس يتمتع بالوصول الفيزيائي إلى حاسب يعمل على إصدار أقدم للنظام Windows، فلا توجد إجراءات أمنية حقيقية تمنعه من العبث بالملفات. أفضل ما يمكنك فعله هو إتباع الإجراءات المضادة التي ناقشناها من خلال الكتاب والتي لا تعتمد على نظام التشغيل. وإذا كنت قلقاً جداً، عليك ترقية النظام إلى نسخة نظام Windows XP/2000 أو محاولة تنصيب نسخة للنظام Linux.

Windows NT/2000/XP

تقدّم عائلة أنظمة التشغيل Windows NT/2000/XP أمناً أفضل بكثير، على خلاف الإصدارات السابقة الموجهة للمستهلك. لكن معظم الإعدادات الأمنية المطلوبة لتقوية النظام ضد المهاجمات لا تكون مفعّلة، افتراضياً. لذلك عليك قضاء بعض الوقت لتعديل الأمن في النظام لضمان أن لديه فرص أكبر لإبعاد الأشرار عنه.



أداة الاستشارة الأمنية الأساسية لشركة Microsoft: (Microsoft's Baseline Security Advisor tool) هي أداة مجانية تفحص تكوينات الأنظمة Windows 2000/XP وتجد حلول لجعلها أكثر أمناً. تتوفر هذه الخدمة من الرابط التالي .www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp

يجب أن تأخذ بعين الاعتبار بعضاً من الإجراءات الأمنية لتقليص فرص اقتحام نظامك وهي (كثير من هذه الخيارات تكون مفعلة وغير مفعلة من خلال إعدادات الأمن المحلية، والتي يمكن أن تصل إليها من خلال كتابة secpol.msc في مربع حوار تشغيل (اضغط زر ابدأ Start ومن ثم زر تشغيل Run)):

- **استخدام التهيئة إلى نظام الملفات NTFS.** لا تقدم أنظمة الملفات FAT و FAT32 أمناً على مستوى الملف أو المجلد، ويمكن الوصول إليها بسهولة باستخدام قرص بدء تشغيل للنظام DOS.
- **إلغاء تفعيل حساب الضيف Guest.** لا تمنح الجاسوس موطئ قدم للنظام حيث يمكنه أن يزيد من امتيازاته.
- **إعادة تسمية حساب المدير.** يعلم الجاسوس الخبير اسم حساب المدير وغالباً سيوجه كامل جهوده لاختراقه، لذا قم باستخدام اسماً مختلفاً لحساب المدير (اسم لا يبدو أنه حساب المدير)، ثم أنشئ حساباً مزيفاً اسمه المدير Administrator بدون أي امتيازات وكلمة مرور صعبة الاختراق. هذا يجعل الجاسوس يهاجم الحساب الخاطئ.
- **منع استعراض اسم المستخدم الأخير الذي قام بتسجيل الدخول.** هناك خيار في قسم خيارات الأمن من السياسات المحلية يمنع ظهور اسم المستخدم الأخير الذي قام بعملية تسجيل الدخول بنجاح إلى النظام، في مربع حوار تسجيل الدخول، وهذا يصعّب مهمة الجاسوس الذي يحاول أن يقوم بعملية تسجيل الدخول يدوياً لأنه يحتاج لتحديد اسم الحساب وكلمة المرور معاً للوصول إلى الحاسب.
- **استخدام سياسات أمنية صارمة.** يمكنك من خلال استخدام قسم سياسة كلمات المرور (Password Policy) ضمن إعدادات الأمن المحلي (Security Settings)، تحديد الطول الأصغر لكلمة المرور، تعقيدها، ومتى يجب تغييرها. يجب أن يكون طول كلمات المرور ثمانية محارف على الأقل، تتضمن مزيجاً من المحارف، الأعداد، والرموز، ويجب تغييرها كل تسعين يوماً على الأقل.
- **تفعيل خيار إقفال الحساب Account Lockout.** يوجد قسم سياسة إقفال الحساب (Account Lockout Policy) ضمن إعدادات الأمن المحلي (Security Settings) والتي تمنع عملية تسجيل الدخول لحساب ما بعد عدد محدد من محاولات تسجيل الدخول الفاشلة (ومع هذا لا يمكنك إقفال حساب المدير Administrator المضمن في النظام). ويحدد إعداد فترة إقفال الحساب (Account Lockout Duration) المدة التي يبقى فيها الحساب في حالة

عدم تفعيل. مثلاً، إذا تم تعيين العتبة إلى القيمة 3 وتعيين المدة إلى 15 دقيقة، فلن يستطيع الجاسوس أن يتوقع كلمات المرور لمدة 15 دقيقة بعد أربع محاولات فاشلة له لتوقع كلمة المرور.

- **تفعيل خيار تسجيل الأحداث Event Logging**. افتراضياً، لا يتم تسجيل بعض الأحداث المتعلقة بالأمن. يجب أن تفعّل هذه الأحداث وتتحقق دورياً من السجلات لمعرفة فيما إذا كان هناك أية محاولات للدخول إلى النظام. تتضمن الأحداث والأنظمة الخاصة بها التي يجب أن تدونها ما يلي:
  - أحداث تسجيل الحساب (نجاح، فشل) Account logon events (success, failure)
  - إدارة الحسابات (نجاح، فشل) Account Management (success, failure)
  - تسجيل الأحداث (نجاح، فشل) Logon events (success, failure)
  - الوصول إلى الكائن (نجاح) Object access (success)
  - تغيير السياسات (نجاح، فشل) Policy Change (success, failure)
  - استخدام الامتيازات (نجاح، فشل) Privilege use (success, failure)
  - أحداث النظام (نجاح، فشل) System events (success, failure)
- **استخدام إجراءات النظام المفتاحي Syskey الأمنية الإضافية**. مع أن التشفير الإضافي المزود مع النظام المفتاحي يحسن أمن تحويلات كلمات المرور، يمكنك زيادة الأمن أكثر من ذلك بطلب كلمة مرور أو قرص مرن لمفتاح بدء تشغيل. عادة، يتم تخزين مفتاح بدء التشغيل للنظام المفتاحي على القرص الصلب، لكن يمكنك تكوين النظام ليحتاج إلى كلمة مرور أو قرص مفتاحي لإلغاء إقفال كلمات المرور قبل أن تبدأ عملية تسجيل الدخول. عليك الانتباه عند استخدام هذه الميزة، لأنك إذا أضعت القرص فلن تتمكن من الإقلاع إلى نظام Windows وسوف يكون عليك إعادة تنصيب كامل النظام.
- **الحذر عند استخدام التلميحات في عملية تسجيل الدخول في النظام Windows XP**. يشكل استخدام تلميح سهل لكلمة المرور خاص بمستخدم معروف اسم حسابه، تهديداً لنظامك.
- **استخدام شاشة توقف محمية بكلمة مرور**. يجب أن تقوم دائماً بتفعيل كلمة المرور لشاشة التوقف لمنع الوصول إلى حاسبك أثناء عدم تواجدك.

يمكنك الحصول على تفاصيل إضافية حول كيفية تفعيل هذه الإعدادات بالإضافة إلى إعدادات أخرى من خلال قسم الأمن على الرابط http://labmice.net، وهو مورد ممتاز لمدراء ومستخدمي أنظمة التشغيل Windows NT/2000/XP.



تتحمل وكالة الأمن القومي الأمريكية NSA (National Security Agency) مسؤولية المحافظة على أمن النظام الحاسبي الحكومي، بالإضافة إلى التجسس. تنشر الوكالة سلسلة من الإرشادات المتعلقة بأمن أنظمة التشغيل Windows NT/2000/XP، والتي تتضمن ملفات ذات اللاحقة inf والتي تنفذ الإعدادات الأمنية المقترحة، تتوفر هذه الإرشادات والملفات من الرابط www.nsa.gov/snac/index.html.

الإجراءات المضادة: الأطول أفضل

بالرغم من أنه يجب أن تستخدم كلمة مرور يبلغ طولها ثمانية محارف على الأقل، إلا أنه من الأفضل استخدام كلمة مرور بطول خمسة عشر محرفاً لعمليات تسجيل الدخول لأنظمة التشغيل Windows 2000/XP. كلما كانت كلمة المرور أطول كلما كان من الأصعب تجاوزها، لكنها تضيف طبقة حماية إضافية في هذه الحالة.

يستخدم نظام التشغيل، في الشبكات المحلية المختلطة المكونة من الأنظمة Windows 3.x/9/x/ME، تحويلات خاصة بإدارة الشبكة المحلية LM (LAN Manager) لجميع الحواسب. من الأسهل اختراق تحويلات مدير الشبكة المحلية LM مقارنة مع طرائق المصادقة الأخرى مثل NTLM و Kerberos، حتى أن كلمة المرور التي يبلغ طولها ثمانية محارف أو أكثر يمكن أن يتم اختراقها بسهولة بسبب ضعف مخطط التحويل لمدير الشبكة المحلية LM.

من ناحية ثانية، هناك خلل في عملية المصادقة الخاصة بالأنظمة Windows 2000/XP: إذا كنت تستخدم كلمة مرور مؤلفة من خمسة عشر محرفاً أو أكثر، يتم تعيين تحويل LM إلى قيمة ثابتة بغض النظر عن كلمة المرور. هذا يجعل نجاح برنامج خدمي صعباً جداً مثل البرنامج LC (في الإصدار LC4، يتم عرض تحويل LM لكلمة مرور يبلغ طولها خمسة عشر محرفاً كتحويل فارغ "empty"). ربما هذا الأمر له علاقة بكون الطول الأعظمي المسموح به لكلمة مرور في نظام التشغيل Windows NT هو أربعة عشر محرفاً، أما في النظامين Windows 2000/XP فالطول الأعظمي هو 127 محرفاً.

كلمات المرور الفعالة

عندما يتعلق الأمر بالمصادقة (أو أي شكل من أشكال الأمن)، لا تلجأ أبداً إلى كلمات مرور سهلة! سيكون حاسبك معرضاً للخطر إذا استخدمت كلمة مرور قصيرة أو سهلة، وستفشل فشلاً ذريعاً إذا أراد أحد ما أن يهاجم حاسبك. انظر قسم "الإجراءات المضادة" في الفصل السادس لمزيد من المعلومات عن مخاطر كلمات المرور السهلة وكيفية اختيار كلمات مرور صعبة.

التشفير

ينبغي تشفير جميع البيانات المهمة على قرصك الصلب. إذا تم التغلب على إجراءات المصادقة الأمنية للنظام BIOS ولنظام التشغيل، يمكنك حماية بياناتك إذا استخدمت تشفيراً قوياً. يزود نظام الملفات المشفر EFS من شركة Microsoft مقداراً لا بأس به من الأمن كما هو مطبق في نظام التشغيل Windows XP Professional – مع أن نظام الملفات المشفر EFS في نظام التشغيل Windows 2000 معرض لعدة أنواع من المهاجمات. انظر قسم "الإجراءات المضادة" في الفصل السادس لمزيد من المعلومات عن التشفير القوي وبعض الاقتراحات عن برامج التشفير الممكن استخدامها.

تلخيص

يشكل النظام BIOS مع نظام التشغيل خط الدفاع الأول ضد الجاسوس الذي يتمكن من الوصول الفيزيائي إلى الحاسب. بالرغم من أنه يمكن اختراق إجراءات النظام الأمنية باستخدام عدد من الأدوات والتقنيات، عليك أن تضمن أن إعدادات الأمن لنظام BIOS ونظام التشغيل لديك مكونة أفضل ما يمكن. هذا الأمر يمنع المتطفلين العرضيين من كشف بياناتك، ويشكل عائقاً أمام الجواسيس المحترفين ليبحثوا عن هدف آخر. لا تركز اهتمامك على المهاجمات عبر الشبكة وتتجاهل نقاط الدفاع الأمنية الفيزيائية والمحلية لحاسبك.



البحث عن الدليل

التجسس الشرعي

مقابل المال يقوم بعض الأشخاص بأعمال التجسس الشرعية على حواسب الآخرين. يتغلغل رجال شرطة الحواسب والفاحصون الشرعيون للحاسب إلى داخل الأقراص الصلبة ووسائط التخزين الأخرى باحثين عن المعلومات والأدلة التي قد تساعد على إدانة أو تبرئة المشتبه به.

يعمل رجال شرطة الحواسب لصالح الوكالات القانونية، قد يكونون ضباط شرطة تحت القسم أو خبراء مدنيون. أما نظرائهم من القطاع الخاص فهم الفاحصون الشرعيون للحواسب والذين يؤدون عملهم لصالح المؤسسات التجارية والمحامين. لا يحتاج الفاحصون الشرعيون أن يحملوا شارة ومسدس، لكنهم يتقاضون أجراً أكثر من رجال الشرطة العاديين.

عليك نسيان خطر الممثل جيمس بوند، المكائد، والغرام في هذا النوع من التجسس. حيث أن الفحص الشرعي للحاسب هو عمل متعب، تفصيلي بشكل مجهد، فقد يتطلب استعراض شاشات متتابعة من الخرج الست عشري من قطاعات القرص الصلب، بحثاً عن الدليل الذي قد يكون موجوداً أو لا يكون بتاتاً. وقد يشكل هذا العمل بالنسبة لرجال الشرطة اكتشاف أعماق النفس البشرية، وخاصة أثناء التحقيقات في جرائم التحرش الجنسي بالأطفال.

نناقش من خلال هذا الفصل كيفية عمل رجال شرطة الحواسب والفاحصين الشرعيين وما هي التطبيقات والتقنيات التي يستخدمونها لاستخلاص المعلومات والدليل. نعرض الإجراءات المضادة المستخدمة لمقاومة محاولات جمع الدليل، بعد تقديم بعض الحيل والأدوات التي يستخدمونها للحصول على المعلومات أو الدليل.

كيف يعمل رجال شرطة الحواسب

يؤدي الفاحصون الشرعيون ورجال شرطة الحواسب نفس العمل: تحديد وجود الدليل على الحاسب المرتبط بنشاط مشبوه أو إيجاد بعض البتات (bits) من المعلومات والتي قد تتحول إلى دليل في نهاية الأمر. بالنسبة للشرطي، فقد يقوم بالبحث عن سجلات مقامرة في الحاسب المحتجز الخاص بمندوب مراهنات الخيل، أما للفاحص الشرعي، فقد يقوم بمحاولات لاستعادة الملفات المحذوفة المرتبطة بفضيحة لشركة محاسبة.

يتبع النوعان من التحقيقات الدعاوى والإجراءات العامة نفسها، يكمن الفرق الأكبر أنه يجب على رجال الشرطة إتباع مجموعة صارمة من القواعد فيما يتعلق بالوصول إلى الحواسب التي قد تتضمن الدليل المطلوب. فعلى سبيل المثال، يحتاج الشرطي رخصة تفتيش من المحكمة للدخول إلى مكتب والبحث عن دليل، بينما يكفي للفاحص الشرعي الذي يعمل لصالح مؤسسة ما، أن يحصل على موافقة رسمية من الشركة ليفتش حاسباً في غرفة موظف.

سوف نركز من خلال هذا القسم على شرطة الحواسب، لكن بما أنه هناك تداخلاً بين المهارات والتقنيات المستخدمة من قبل كلا رجال شرطة الحواسب والفاحصين الشرعيين، يمكنك تطبيق الكثير من المعلومات القادمة على الفاحصين الشرعيين أيضاً.

في البداية يمكن أن نشير إلى أن مستوى المهارة والقوة التقنية لشرطة الحواسب، يمكن أن تختلف اختلافاً كبيراً. يستطيع القليل من رجال شرطة الحواسب أن يطبقوا مبدأ الهندسة العكسية[1] على خدمة التشفير، بينما يعتمد الآخرون كلياً على الأدوات البرمجية للفحوصات الشرعية لأنظمة التشغيل Windows الجاهزة للاستعمال. هنا نجد أن معظم رجال شرطة الحواسب كانوا رجال شرطة بالأصل ولم يلتحقوا بقوى القانون ولديهم خلفية تقنية. (لكن تستخدم الوكالات القانونية أشخاصاً ذوي مهارات تقنية وليسوا ضباطاً تحت القسم، والذين قد يملكون شهادات متعلقة بالتقنية والخبرة الصناعية، كما يتمتع الفاحصون الشرعيون الخاصون بخلفية تقنية أكبر من أمثالهم رجال شرطة الحواسب. كما تقوم بعض الوكالات الحكومية، بسبب القضايا المتراكمة، باستخدام شركات استشارية خاصة لتقوم بعملية البحث عن الدليل الحاسبي).



نشرت وزارة العدل، في شهر حزيران (يونيو) من عام 2001، مرجعاً متميزاً يدعى التحقيق في مشهد الجريمة الإلكترونية: دليل للمبتدئين. هذا الدليل السهل والقصير موجه خصيصاً لضباط قوى القانون غير التقنيين، ولكنه يتضمن أيضاً معلومات لا بأس بها للقراء الذين يتمتعون ببعض الخبرة التقنية. يتوفر هذا الدليل على الرابط التالي www.ncjrs.org/pdffiles1/nij/187736.pdf.

[1] الهندسة العكسية Reverse Engineering: طريقة لتحليل منتج ما بحيث تتم دراسة الشكل النهائي له وتحديد مواصفاته من أجل تحديد مكوناته فيما بعد.

بسبب عدم تمتع معظم رجال شرطة الحواسب بخلفية تقنية قوية، توجد مجموعة من المصادر الحكومية والخاصة والتي تقدم تدريباً للفحوص الشرعية للحواسب وبرامج للحصول على شهادات. الشهادة مهمة جداً لتأسيس المصداقية على منصة الشهود، لأنه غالباً ما يشهد رجال الشرطة في المحكمة.

يسعى رجال شرطة الحواسب للعمل ضمن مكاتب ومخابر تتضمن تجهيزات وبرمجيات متخصصة في عملية البحث عن الدليل. في الماضي القريب، كانت الوكالات البلدية الفدرالية الكبيرة فقط، مزودة ومجهزة بفرق وتجهيزات خاصة بالتحقيقات الحاسبية، لكن الآن وبعد أن أصبحت الحواسب الشخصية جزأ من الحياة اليومية، حتى الأقسام الحكومية الصغيرة تخصص جزءً من ميزانيتها لرجال شرطة الحواسب ذوي دوام كامل أو جزئي وبالتجهيزات المناسبة.

على خلاف الجواسيس الآخرين، لا يقلق رجال الشرطة حول كونهم خفيين قليلاً، ما لم يتورطوا بأعمال الحقيبة السوداء (دخول سري لعقار ما مصدق من قبل المحكمة من أجل الحصول على دليل). حيث يملكون مسبقاً الوصول إلى تجهيزات وبرمجيات المشتبه به ويكونون مهتمين بشكل أساسي باكتشاف دليل ما يربط المشتبه به بالجريمة.

هناك طلب كبير على خدمات رجال شرطة الحواسب (والفاحصين الشرعيين أيضاً)، وربما لن يكفي العرض الطلب في السنوات القادمة، ومع ذلك تدرك الوكالات القانونية أهمية رجال الشرطة المدربين القادرين على استخلاص معلومة رقمية من الجريمة، لكنهم يواجهون بمجموعة من التحديات المستقبلية والتي ستبعدهم أكثر عن الجو، نعرض فيما يلي بعضاً من هذه التحديات:

- **أقراص صلبة أكبر.** كلما زاد حجم القرص الصلب، زاد عدد البايتات الواجب تفتيشها والبحث ضمنها. حيث أصبحت الأقراص الصلبة، التي يتراوح حجمها من 100–200 جيغابايت، شائعة ويمكن شرائها، يستغرق نسخ القرص الصلب الخاص بالمشتبه به وقتاً أطول، ويستغرق البحث عن الدليل وقتاً أطول، وتحتاج لوسائط تخزين إضافية للاحتفاظ بالدليل. تتطلب جميع هذه الإضافات ميزانية أكبر.
- **عدد القضايا المتزايد.** يستخدم الحاسب بشكل متزايد في جميع أنواع الجرائم. حيث كان على رجال الشرطة، منذ عشر سنوات، أن يقلقوا حول المخربين والمجرمين ذوي الرواتب فقط، أما اليوم يفترض على رجال الشرطة نفسهم أن يبحثوا عن الدليل للجرائم المرتبطة بالمخدرات، جرائم القتل، محاولات الانتحار، الاحتيال، وأي جريمة أخرى يتواجد فيها جهاز الحاسب.

- **المجرمون العباقرة تقنياً**. أشارت الإحصائيات أن نسبة سكانية معينة سترتبط بالجريمة، وبالتالي بما أن الجيل النامي سيكون مثقف حاسبياً أكثر من قبل، فبالتالي هؤلاء الذين سيسلكون درب الإجرام سيكونون على إطلاع على تقنيات تعوق أو تتحدى التحقيقات القانونية.

يتضمن عمل رجال شرطة الحواسب الكثير من العوامل، ويمكن أن نقسمها إلى ثلاثة عوامل أساسية: الحجز على الممتلكات، النسخ الشرعي، والفحص. ستقوم بامتحان كل منها.

مضبوط: مختبرات محلية للفحوصات الشرعية للحاسب

افتتح مكتب التحقيقات الفدرالي، في شهر تشرين الثاني (نوفمبر) عام 2000، المختبر المحلي الأول للفحوصات الشرعية للحواسب RCFL (Regional Computer Forensics Laboratory) في مدينة San Diego في ولاية California. تم إعداد المختبر ليكون متعدد الوكالات ومتعدد السلطات القضائية ويضم 18 شرطياً حاسبياً من وكالات مختلفة جاهزون للتحقيق في الجرائم المرتبطة بالحواسب في منطقة San Diego. عالج المختبر في السنة الأولى ما يقارب 400 قضية وشجع على افتتاح مختبرات أخرى في أرجاء البلاد.

فيما يلي بعض القضايا التي ساعد المختبر في San Diego أن يجمع الأدلة لها:

- قضية Michael Craig Dickman، والذي حكم بسجنه لمدة تسع سنوات لقيامه بنهب 12 مصرفاً محلياً. حيث وجد المحققون الشرعيون للحواسب نسخاً من ملاحظات السرقة الخاصة بالمدير التنفيذي السابق لتقنية استخدام العمليات الحيوية في الصناعة أعطاها للرواة على شكل ملفات طباعة محذوفة على حاسب محمول، حيث طلب من أخته أن تخرجه من شقته.
- قضية Arthur Gerardo و Valerie Beidler. تمت إدانتهما بتهمة تعذيب وقتل شريك بالسكن والذي ساعدهما على تلفيق شيكات وتزوير هويتهم الشخصية. تضمن الحاسب المحتجز صور الشيكات ورخص القيادة والتي تم سحبها وتعديلها رقمياً.
- قضية Charles Andy Williams. وهو مراهق، تمت إدانته بتهمة قتل طالبين وجرح ثلاثة عشر آخرين في مدرسة Santana الثانوية في شهر آذار (مارس) من عام 2001. تمت احتجاز حاسب William كجزء من التحقيقات.
- قضية David Westerfield. أدين بتهمة خطف وقتل جاره الصبي Danielle van Dam البالغ من العمر سبع سنوات. تضمن حاسب David حوالي 64,000 صورة و2,200 مقطعاً فيديوياً (تم استعادة 85 صورة لفتيات ومراهقين فتيان مغتصبين).

إجراءات مضادة: الحصول على شهادة

نعرض فيما يلي بعضاً من أكثر المزودين شهرة لتدريبات التحقيقات الحاسبية والشهادات:

- **الجمعية العالمية لخبراء التحقيقات الحاسبية IACIS (International Association of Computer Investigative Specialist)**. وهي منظمة لا ربحية خاصة بمحققي قوى القانون المتعلقة بالحواسب. إن تدريباتها وشهاداتها معروفة بشكل كبير. لمزيد من المعلومات عن هذه المنظمة اتبع الرابط www.cops.org.
- **جمعية التحقيق في جريمة التكنولوجيا المتطورة HTCIA (High Technology Crime Investigative Association)**. وهي منظمة تجارية مكونة من المحققين المدنيين والتابعين لقوى القانون. تملك المنظمة فصولاً محلية وتقيم مؤتمرات وأحداثاً تدريبية. لمزيد من المعلومات عن هذه المنظمة اتبع الرابط www.htcia.org.
- **المركز الوطني لجرائم الفئات العالية المستوى NWCC (National White Collar Crime Center)**. يزود المركز تدريباً مجانياً للاختبارات الشرعية الحاسبية للموظفين في قوى القانون، كما يقدم المركز دورات دراسية متنوعة تدرس في جميع أرجاء أمريكا. لمزيد من المعلومات اتبع الرابط www.cybercrime.org.
- **شركة التقنيات الجديدة New Technologies Inc**. وهي مصنّع برمجيات تجارية للاختبارات الشرعية في ولاية Oregon والتي تقدم أيضاً تدريباً لقوى القانون والمدنيين أيضاً. لمزيد من المعلومات عن هذه المنظمة اتبع الرابط www.forensics-intl.com.

الحجز على الممتلكات

قبل أن تتمكن من البحث عن دليل على الحاسب، من الواضح أنك تحتاج أولاً أن تصل إلى هذا الحاسب، وهذا يعني عادة حجز الحاسب وأي مواد أخرى إلكترونية أو غير إلكترونية والتي قد ترتبط بالقضية. (قد يتدخل الفاحصون الشرعيون في حالات نادرة بعملية حجز الحواسب).

يمنع الدستور قيام قوى القانون بحجز الممتلكات حينما يعتقدون أنه تم ارتكاب الجريمة، قبل القيام بعملية الحجز يجب أن يوافق القاضي على مذكرة التفتيش. في حالة التعامل مع الحواسب، يكتب شرطي الحواسب مذكرة التفتيش أو يساعد في صياغتها. يجب أن تكتب مذكرات التفتيش بدقة لتتمكن من المثول في المحكمة خلال مقاضاة المتهم، لذلك يجب على شرطي الحواسب أن يصرح بوضوح عن الأجهزة والحواسب التي سيتم تفتيشها، مع سبب محتمل لفحصها.

يتم تنفيذ مذكرة التفتيش بعد الحصول على الموافقة. حسب الجريمة التي نتعامل معها، يمكن أن يكون التفتيش هو دخول عادي من الباب، أو اقتحام مسلح في ساعات الصباح الباكرة.

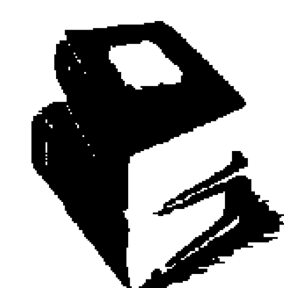
بما أنه لا يتم التفتيش في مكان الحجز، يجب على رجال الشرطة إتباع مجموعة من الخطوات عند احتجاز الحواسب والأدلة الإلكترونية، نعرض فيما يلي الخطوات وبعض الإرشادات التي تحتاجها الشرطة:

- **تأمين المكان.** إبعاد جميع الأشخاص عن منطقة التفتيش حيث سيتم جمع الأدلة. إذا كان الحاسب يعمل، اتركه يعمل. إذا كان مطفئاً، لا تقم بتشغيله. (إذا كان الحاسب يعمل، يتم تسجيل محتويات الشاشة، ويتم سحب كبل الطاقة عادة من الحاسب، وليس من الجدار).
- **حماية البيانات الزائلة.** يجب تأمين وتوثيق أي أداة تقوم بتخزين البيانات في ذاكرة تعمل على البطاريات (أجهزة النداء Pagers، الهواتف الخلوية Cell phones، وغيرها).
- **التعرف على خطوط الهاتف وكابلات الشبكة المتصلة بالحاسب.** توثيقها، فصلها من الجدار، وتصنيف جميع الكابلات.
- **إدارة المقابلات التمهيدية.** بعد الفصل بين جميع الأشخاص في المنطقة والتعرف عليهم (شهود، مشتبهين، أو أشخاص آخرين)، عليك طرح الأسئلة وتوثيق المعلومات حول ملكية الحاسب، كلمات المرور، وأي أجهزة أمنية، عليك أيضاً أن تكتشف فيما إذا كانت البيانات تخزن خارج هذه المنطقة. (إنه لأمر مدهش كمية المعلومات التي يمكنك أن تحصل عليها من الأشخاص).
- **توثيق المكان.** قبل أن تقوم بفحص أو نقل أي شيء، عليك التقاط صور فوتوغرافية أو تسجيل المكان بكامله على الفيديو، بما فيها الحاسب، الشاشة، وأية طرفيات أخرى. يمكنك تدوين بعض الملاحظات بالإضافة إلى الصور.
- **الحصول على الدليل.** يمكن أن يكون الدليل بصورة إلكترونية أو غير إلكترونية، حيث يجب جمع الأوراق، الملاحظات، كلمات المرور، كتيبات الاستخدام، أو مستندات مرتبطة بالجريمة. اسحب كبل الطاقة من الحاسب، وفي حالة وجود حاسب محمول أزل البطارية (وذلك لمنع أي مصيدة برمجية مفخخة والتي قد تحذف البيانات خلال إجراء إيقاف التشغيل العادي). ضع قطعاً من الشريط على مقابس المحركات ومخرج الكهرباء. دوّن مصنّع، نموذج، والرقم التسلسلي للحاسب.
- **حزم الدليل ونقله.** يجب تصنيف وجرد جميع الأدلة التي تم الحصول عليها، كما يجب تسمية جميع الكابلات لتوافق المقابس التي يتم إدخالها إلى الحاسب (مثلاً، ضع التسمية "M"

على منفذ الفأرة وضع نفس التسمية "M" على كبل الفأرة) وفي حال وجود عدة حواسب، تأكد من تسمية الطرفيات والكابلات بحيث تتوافق مع الحاسب الذي كانت متصلة به. يجب وضع أي وسائل مغناطيسية في أكياس أو حقائب بلاستيكية مقاومة للكهرباء الساكنة، كما عليك حماية التجهيزات، خلال عملية نقل الدليل، من الصدمات والاهتزاز الزائد، كما يجب أن تتجنب التعرض للحقول المغناطيسية (أجهزة الراديو، مغناطيس مكبرات الصوت، أو المقاعد الساخنة)، الحرارة المرتفعة، البرد، أو الرطوبة.

- **تخزين الدليل.** تملي سياسة الأقسام الحكومية كيفية تخزين الدليل، لكن من الهام حماية الحاسب والطرفيات الأخرى من الحرارة، الرطوبة، البلل، الغبار، والمصادر المغناطيسية. في إحدى قضايا قتل طفل ذو مركز هام، تم تخزين الدليل في سرداب مكتب البريد، وبعد وقوع عدة فيضانات، صدئت الحواسب وتعفنت الأقراص المرنة.

بعد الانتهاء من عملية حجز الدليل، نقله، وتخزينه، العمل الذي يقوم به الشرطي هو مضاعفة جميع وسائط التخزين المرتبطة بالقضية.



يتوفر دليل "البحث واحتجاز الحواسب والحصول على الأدلة الإلكترونية خلال التحقيقات الجنائية" الخاصة بوزارة العدل الأمريكية على الرابط www.cybercrime.gov/s&smanual2002.htm.

أساليب: تسلسل الملكية

تسلسل الملكية أو (تسلسل الحراسة) هو عبارة عن مفهوم حرج في التحقيقات الجنائية والمدنية، ومعناه ببساطة وجود سلسلة متصلة تقوم بتوثيق جميع الأشخاص الذين كانوا يملكون الدليل من وقت الحصول عليه حتى وقت تخزينه. الهدف من تسلسل الملكية هو ضمان المسؤولية بين هؤلاء الأشخاص الذين كانوا يتعاملون مع الدليل لتخفيض التأثير على الشواهد بالرشوة أو الترهيب. وهذا الأمر حرج بشكل خاص عند التعامل مع الحواسب، حيث يمكن تعديل الدليل الرقمي بسهولة.

يتم توثيق تسلسل الملكية باستخدام سجلات تتعقب أثر الذين حصلوا على الدليل، التسميات التي تميز بوضوح أجزاء الدليل، ومكان التخزين السري للأدلة.

المضاعفة الشرعية

قبل أن يقوم شرطي الحواسب بفحص الحاسب، يقوم بمضاعفة شرعية للقرص الصلب وأي وسائط تخزين أخرى تم احتجازها كدليل. القاعدة الجوهرية أثناء الاختبارات الشرعية الحاسبية هي عدم إجراء الاختبار على وسائط التخزين الأصلية، إنما استخدام نسخة مطابقة تماماً للأصل، يتم هذا لسببين:

- قد تعدّل الملفات المفتوحة الدليل بشكل غير متعمد، أثناء البحث في القرص الصلب عند تشغيل النظام Windows، حتى يمكن أن تؤدي عملية إقلاع النظام Windows إلى تغيير بعض الملفات.
- بما أنه يمكن تغيير البيانات الرقمية بسهولة، فقد يثير القاضي مسألة التأثير المحتمل على الشواهد إذا تم فحص الوسائط الأصلية مباشرة واستخدمت كدليل وحيد.

يمكن أن تتم عملية المضاعفة في مكان حجز الدليل أو في مكتب الوكالة أو المختبر، يفضل معظم رجال الشرطة العمل في المكتب حيث يملكون جميع الأدوات والتجهيزات المناسبة، يمكن أن تتم المضاعفة في مكان حجز الدليل تحت ظروف خاصة، مثل أعمال الحقيبة السوداء.

يجب إتباع الإجراءات التالية، لضمان صلاحية الدليل ووقوفه في المحكمة:

1. قم بإقلاع الحاسب المطلوب باستخدام نظام تشغيل آخر، مثل النظام DOS أو النظام Linux، ثم استخدم مجموعاً تدقيقياً أو تطبيقاً لتحويل آمن (مثل التحويل SHA-1 أو MD5) لإنشاء عناوين الملفات والمجلدات. (إن استخدام نظام تشغيل آخر يمنع النظام Windows من تغيير الملفات عند بدء التشغيل).
2. استخدم تطبيقاً يعمل ضمن نظام التشغيل DOS أو Linux لإنشاء نسخة مماثلة للقرص الصلب (يتم عرض بعضاً منها في فقرة " أدوات تجميع الدليل" من هذا الفصل). يجب إنشاء هذه النسخة على وسائط عقيمة (قرص صلب جديد أو شريط) أو الوسائط التي تم "مسحها" لضمان عدم وجود أي بيانات متبقية.
3. بعد الانتهاء من عملية النسخ، استخدم المجموع التدقيقي أو برنامج التحويل للتأكد من أن النسخة مطابقة للأصل.
4. تأكد من توثيق كامل العملية ومن ثم قم بتخزين القرص الصلب الأصلي في مكان آمن.

الخطوة التالية هي البدء بالبحث عن الدليل على القرص الصلب المنسوخ، ويتم استخدام الإجراءات نفسها لمضاعفة الوسائط الأصلية قبل إنجاز الفحص، عند وجود دليل محتمل على وسائط تخزين أخرى، مثل الأقراص المرنة، الاسطوانات المضغوطة، أو الأشرطة.



توجد عدة شركات مصنعة لمحطات العمل Workstations مصممة خصيصاً لمضاعفة الأقراص الصلبة وتحليل الاختبارات الشرعية الحاسبية، تتضمن محطات العمل هذه ميزات مثل حجرات متعددة للقرص الصلب، تجهيزات مختلفة لوسائط التخزين، وحزمة برمجيات خاصة للاختبارات الشرعية. يمكننا أن نذكر من المصنعين الأساسيين، الاستخبارات الرقمية Digital Intelligence (www.digitalintel.com)، DIBS USA (www.dibsusa.com)، والحواسب الشرعية Forensics Computers (www.forensic-computers.com).

الاختبار

يبدأ شرطي الحواسب بعملية الاختبار بعد مضاعفة الوسائط، و يتضمن هذا الاختبار عادة وصل القرص الصلب المضاعف إلى محطة العمل المخصصة لهذه الاختبارات. (تتم عملية إقلاع الحاسب المحتجز باستخدام قرص مرن للوصول إلى معلومات الرقاقة CMOS الهامة لمعرفة تواريخ وأوقات إنشاء الملفات أو تعديلها، لكن الأهم من ذلك هو منع إقلاع الحاسب من القرص الصلب بسبب إمكانية تعديل الملفات). تتضمن محطة العمل هذه برمجيات تحليل وتستخدم بشكل مثالي للتعامل مع الدليل المشكوك به.

تتضمن المهام الأساسية الواجب القيام بها في الاختبار الشرعي، بغض النظر عن وسائط التخزين ما يلي:

- **فحص النظام**. يجب فحص سجل الإقلاع وملفات تكوين النظام (مثل الملفات، Config.sys، Autoexec.bat، أو قيم تسجيل النظام).
- **استعادة الملفات المحذوفة**. يجب استعادة جميع الملفات المحذوفة. (يجب تغيير الحرف الأول لاسم أي ملف مسترجع من الست عشري E5 إلى أي محرف فريد آخر لتحقيق الانسجام، تتم مناقشة هذا في فقرة ثانية من هذا الفصل).
- **استعراض الملفات**. يتم تسجيل قائمة بالملفات في وسائط التخزين، سواء تضمنت الدليل أم لا.
- **فحص المساحة غير المخصصة**. يتم إجراء بحث ضمن المساحة غير المخصصة عن أي ملفات.
- **فحص المساحة المهملة**. يتم إجراء بحث ضمن المساحة المهملة (المساحة غير المستخدمة ضمن وسط التخزين) عن أي دليل.
- **فحص الملفات**. يتم فتح واستعراض ملفات المستندات.

- **فك تشفير الملفات المشفرة.** يجب محاولة فك تشفير أية مستندات مشفرة، واستعراض المحتويات عند النجاح.
- **التوثيق الكامل.** يتم إنشاء نسخة مطبوعة لأي دليل، وتوثيق عملية الاختبار كاملة.

توجد طريقتان لتنفيذ عملية الاختبار الشرعي. يستطيع الشرطي إنجاز جميع هذه المهام باستخدام خدمات برمجية متنوعة أو يستطيع استخدام برنامج مؤتمت لتحليل وتجميع الدليل، والذي بالتأكيد أسرع وأسهل للاستخدام. سوف نستعرض عدداً من التطبيقات المستخدمة لاختبارات الحاسب الشرعية ضمن فقرة " أدوات تجميع الدليل" من هذا الفصل. على أية حال، يتم تطبيق العملية نفسها لكل اختبار وهذا يضمن الانسجام أثناء التحقيقات.

تجدر الإشارة إلى نقطة هامة تتعلق بطور الاختبار هي أن الشرطي سيبحث عن دليل معين مرتبط بجريمة معينة، فقد يعثر بالصدفة على دليل إضافي يربط المشتبه به بنشاطات إجرامية أخرى، لكنه سيوجه تركيزه على الدليل الذي يربطه بأي جريمة موجهة ضده.

يكتب الشرطي تقريراً بنتائج البحث بعد الانتهاء من عملية الاختبار. تعتمد مدة العملية على صرامة وأهمية الجريمة والعمل المتراكم على الدليل الإلكتروني الذي يجب أن يتقدم عن القضايا الأخرى. إنه لأمر اعتيادي أن تستغرق المختبرات المحلية الجنائية أشهراً كثيرة في عملية الاختبار نتيجة الأعمال المتراكمة وذلك بسبب عدم توفر الموارد لدى وكالات الشرطة الصغيرة لتقوم بهذا العمل.

إذا انتقلت القضية إلى المحكمة، فعلى الأرجح أن شرطي الحواسب سيمثل أمام المحكمة بصفته شاهداً أمام القضاء، كما أن مهمة شرطي الحواسب المتمثلة بشرح المصطلحات التقنية المعقدة أمام هيئة المحلفين بأسلوب واضح وسهل، ليست بالمهمة السهلة إنما هي مهمة حرجة مثل مهمة اكتشاف الدليل على القرص الصلب. كما أنه قد تتم المواجهة بين شرطي الحواسب والفاحص الشرعي الخاص الذي يمثل الدفاع في المحكمة، والذي قد يحاول إثارة الشكوك حول مصداقية الشرطي فيما يتعلق بالطريقة التي يتم فيها فحص واختبار الدليل.

أساليب الجواسيس

حان الوقت لتلعب دور الجاسوس مرة أخرى، لكنك الآن سترتدي قبعة الخير. تخيل نفسك شرطياً تحرياً يعمل على قضية خطرة، قد تكون جريمة اختطاف طفل أو جريمة قتل. لقد تم احتجاز حاسب المشتبه به والآن حان دورك لتبحث عد دليل يفيد القضية. (حالياً يجب أن تركز على محتويات الحاسب ولا تقلق حول الاختبارات المتعلقة بالشبكات. سوف نناقشها في الفصل العاشر).

سوف نفترض أنك قمت بمضاعفة القرص الصلب وتجري اختباراتك حالياً على النسخة الاحتياطية، سوف تتحقق يدوياً من بعض المواقع ضمن القرص الصلب حيث يمكن أن يتواجد الدليل.

استغلال نقاط الضعف

يمكن تشبيه الحاسب بمنخل مثقوب فيما يتعلق بتخزين المعلومات والدليل (تحدد البيانات الإلكترونية "برسائل" أو "تسجيلات" بموجب القانون الفدرالي للدليل 1001، والذي يشمل البيانات المخزنة بالنبض المغناطيسي أو التسجيل الكهربائي). توجد أماكن كثيرة جداً للبحث عن البيانات التي يمكن أن تشكل الدليل والمرتبطة بقضيتك. مثالياً، عليك أخذ الحاسب إلى مكتبك أو مختبرك، حيث يمكنك أن تضاعف القرص الصلب وأن تبدأ البحث عن الدليل. فيما يلي بعض الأماكن حيث يجب أن تبحث وعما يجب أن تبحث.

الملفات

من الواضح أنك لست بحاجة إلى شهادة جامعية لتعرف أنك ستفحص محتويات مستندات محددة، فعلى سبيل المثال، الملفات التالية 2002drugdeals.doc، nudekids.jpg، أو secretevilplans.xls ستسترعي انتباهك على ما أظن وستفتحها، معتمداً على ما تبحث عنه.

لكن عندما يتعلق الأمر بالدليل، هناك أكثر بكثير من مجرد فحص محتويات المستندات. من بعض الدلائل القيمة المتعلقة بالملفات ما يلي:

أوقات التحكم بالوصول MAC Times: يحفظ نظام التشغيل Windows الأوقات التي تم فيها تعديل الملف، الوصول إلى الملف لآخر مرة، وتعديل الملف، وتُعرف بأوقات التحكم بالوصول MAC Times ويمكنك أن تستعرضها ضمن مستكشف Windows وذلك عن طريق تحديد الملف ثم عرض خصائصه. تظهر أهمية ملفات أوقات التحكم بالوصول عند جمع الأدلة لأنها تعطي تاريخاً موجزاً للملف. مثلاً، إذا أدلت جاسوسة مشتبه بها بتصريح بأنها قد قامت بتحميل ملف الميزانية بالصدفة بتاريخ ووقت محدد لكنها لم تفتحه أبداً، تستطيع أوقات التحكم بالوصول إلى هذا الملف أن تكشف فيما إذا كانت تكذب أو تقول الحقيقة.

الاختصارات SHORTCUTS: الاختصارات هي مراجع للتطبيقات، الملفات، أو الأجهزة (الطابعات، أجهزة التخزين الخارجية، وأجهزة الشبكة). تملك الاختصارات اللاحقة LNK. لكن نظام التشغيل Windows يخفيها عن المستخدم بحيث يظهر اسم اللاحقة فقط على سطح المكتب أو ضمن مستكشف Windows. تم تصميم الاختصارات لتوفر الوقت، مثلاً تستطيع مندوبة

مبيعات إنشاء اختصار يشير إلى لائحة زبائن تستخدمها بكثرة، فهي توفر الوقت بالضغط على الاختصار بدلاً من اجتياز مجلدات كثيرة للوصول إلى هذا الملف.

يحفظ نظام التشغيل Windows مجموعة من الاختصارات الإضافية، عدا اختصارات المستخدمين، في عدة أماكن، بشكل خاص في المجلدات التالية سطح المكتب، المستندات الأخيرة، قائمة ابدأ، وإرسال إلى.

- **سطح المكتب.** يخزن هذا المجلد جميع الاختصارات التي تظهر على سطح المكتب.
- **المستندات الأخيرة.** يتضمن مجلد المستندات الأخيرة اختصارات الملفات المفتوحة حديثاً والتي تظهر ضمن بند قائمة المستندات عند النقر على زر ابدأ.
- **قائمة ابدأ.** يتضمن هذا المجلد اختصارات إلى التطبيقات التي تظهر ضمن بند قائمة البرامج عند الضغط على زر ابدأ.
- **إرسال إلى.** يتضمن مجلد إرسال إلى اختصارات إلى التطبيقات والأجهزة التي يستطيع المستخدم إرسال البيانات إليها، مثل محرك الأقراص المرنة أو تطبيق للبريد الإلكتروني.

تتوضع هذه المجلدات في أنظمة التشغيل Windows 9x/ME في مجلد Windows، أما في أنظمة التشغيل Windows NT/2000/XP في مجلدات Documents And Settings.

يمكن أن تكون الاختصارات هامة جداً لجمع الأدلة للأسباب التالية:

- قد تدل الاختصارات التي تشير إلى جهاز أو شبكة خارجية إلى وجود أدلة إضافية غير التي تكون ضمن القرص الصلب.
- قد تزود الاختصارات ضمن قائمة ابدأ دليلاً عن تثبيت تطبيق محدد على الحاسب في وقت ما.
- تستعرض الاختصارات الموجودة ضمن مجلد المستندات الأخيرة معلومات حول المستندات المفتوحة حديثاً، بالرغم من أنها قد تكون محذوفة.
- تحتوي الاختصارات أوقات التحكم بالوصول للملفات التي تشير إليها كجزء من البيانات للملف LNK.، وخاصة عند انزياح البايتات التالية 28، 36، و 44.

المجلدات والملفات المخفية: يحاول بعض مستخدمي الحواسب الذين يعتقدون بأنهم أذكياء جداً بإخفاء الدليل بتعيين سمة الملف أو المجلد لتكون مخفية. الهدف الأصلي للملفات أو المجلدات المخفية أو غير المرئية هي إخفاء ملفات النظام من المستخدمين الذين لا يحتاجون للوصول إليها، لكن أي مستخدم يمكنه جعل الملف أو المجلد مرئياً.

في مستكشف Windows، اضغط بزر الفأرة اليمين على الملف أو المجلد ثم قم باختيار الخصائص من القائمة المنبثقة لعرض السمات، إذا تم اختيار سمة الإخفاء Hidden لن يتم عرض الملف أو المجلد ضمن مستكشف Windows أو عند عرض مربع حوار فتح الملف.

يفترض مستخدمو الحاسب المبتدئون بدون الفهم التام لكيفية عمل نظام الملفات، بأنه يمكنهم الاستفادة من هذه الميزة لإبعاد الأشخاص المتطفلين عن مستنداقم. لسوء الحظ، لم يقوموا بهذا بنوايا سيئة، حيث يمكن عرض الملفات والمجلدات المخفية بعدة طرائق:

- **مستكشف Windows**. الخيار الافتراضي ضمن مستكشف Windows هو عدم عرض الملفات والمجلدات المخفية، لكن يمكن تغيير هذا الخيار بسهولة من خيارات المجلد لعرض كافة الملفات.
- **سطر الأوامر**. لا يظهر الأمر dir الخاص بالنظام DOS ضمن جلسات العمل على سطر الأوامر الملفات المخفية، لكن الأمر dir /a يظهر جميع الملفات.
- **التطبيقات**. يمكن اكتشاف الملفات والمجلدات المخفية بسهولة عن طريق التطبيقات الخاصة بالاختبارات الشرعية للحواسب، أو عن طريق برامج أخرى مبرمجة خصيصاً لاستعراض كل ملف ومجلد بغض النظر عن سماته.

قد تبقي الملفات والمجلدات المخفية الجاسوس العرضي بعيداً والذي يعبث فقط، لكنها لن تقف في وجه أي شخص جاد في البحث عن الدليل.

الملفات المؤقتة: يستخدم نظام التشغيل Windows والتطبيقات الأخرى الملفات المؤقتة استخداماً واسعاً، وهي ملفات يتم إنشائها وحذفها من قبل التطبيق ودون علم من المستخدم، يتم إنشاء هذه الملفات عادة كجزء من عملية حفظ الملف ويمكن أن تتضمن جميع أنواع الملفات المشوقة التي قد تكون مفيدة كدليل. فعلى سبيل المثال، تسمى الملفات المؤقتة التي ينشئها برنامج Microsoft Word بالاسم ~WRLxxxxxx.tmp ويمكن إعادة تسميتها لتأخذ اللاحقة DOC. لتتمكن من فتحها مباشرة من برنامج Word.

تتوضع الملفات المؤقتة نموذجياً في:

- مجلد temp ضمن مجلد Windows
- أي مجلد يحتوي التطبيق أو الملف المنشأ من قبل التطبيق.

لا تقوم الكثير من التطبيقات بحذف الملفات المؤقتة، وتظهر هذه الملفات بوضوح ضمن مستكشف Windows، غالباً ذات اللاحقة TMP.، لكن يمكن استرجاع الملف المؤقت المحذوف باستخدام برنامج استرداد.

إذا قمت بالبحث عن الملفات المؤقتة ذات اللاحقة TMP. و لم تجد أي ملف، فعلى الأرجح يستخدم مستخدم الحاسب برنامج للتخلص من الأدلة (سوف نناقش هذا البرنامج بتفصيل أكبر لاحقاً في هذا الفصل). يوجد احتمال آخر هو تعيين المتحولات البيئية[1] المؤقتة للنظام TMP وTEMP لتشير إلى القرص RAM (قرص موجود في الذاكرة تختفي محتوياته عند إطفاء الحاسب). أو لتشير إلى مجلد مشفر. في هذه الحالة ستختفي الملفات المؤقتة عند إطفاء الحاسب أو تخزن في قرص محمي بكلمة مرور والذي يجب إدخاله إلى محرك القرص للوصول إلى الملفات.

لواحق الملفات المتغيرة: تظهر لواحق الملفات (وهي الحروف الثلاثة بعد النقطة في اسم الملف) ما هو نوع المستند، مثلاً DOC. هو ملف Microsoft Word، XLS. هو ملف ورقة عمل Microsoft Excel، وBMP. هو ملف صورة بتات.

يحاول الأشخاص أحياناً بإخفاء الدليل معتقدين أنه بإمكانهم إخفاء المعلومات التي يحتويها الملف فعلياً بتغيير لاحقته، هذا أسلوب شائع يستخدم من قبل هواة جمع صور الأطفال الخلاعية محاولين إخفاء الملفات التي لاحقتها JPG. أو GIF..

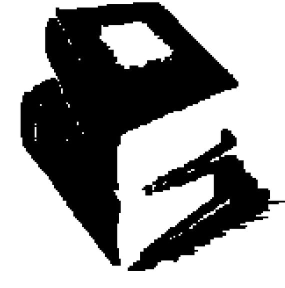
لنتأكد من أنها طريقة غير فعالة، استخدم برنامج الرسام مثلاً لإنشاء ملف صورة وخزنه باسم SPY.JPG، ثم استخدم مستكشف Windows لتغيير لاحقة الملف إلى SPY.INI. لن يحزر أحد اعتماداً على الاسم والأيقونة بأن هذا الملف هو ملف صورة.

والآن استخدم برنامج الرسام لتفتح الملف SPY.INI، لا يستبعد البرنامج الملف مباشرة فقط لكون لاحقته INI.. يتحقق برنامج الرسام بدلاً من ذلك من محتويات الملف وفيما إذا تضمن معلومات تعرّفه كملف صورة وإذا وجد هذه المعلومات، يفتح الملف بنجاح.

تملك جميع المستندات تنسيقاً فريداً، فيما عدا الملفات النصية البسيطة. ويتضمن هذا التنسيق معلومات ترويسة الملف والتي تسمح للتطبيقات أن تتعرف على تنسيق ملف محدد بحيث إما تقوم بفتح الملف أو تستعرض رسالة خطأ تفيد بعدم القدرة على قراءة الملف. من السهل جداً برمجة تطبيق يستعرض مجلدات القرص الصلب، ويظهر الملفات التي تتضمن ترويسة محددة بغض النظر عن لاحقة هذه الملفات. يمكن أن تجد هذه الميزة في عدة تطبيقات تجارية خاصة بالاختبارات الشرعية.

يجب أن يتم التحقق من الملفات التي قد تم تغيير لواحقها عندما يمتلك المشتبه به معرفة حاسبية فوق متوسطة.

[1] متحول البيئة: متحول يستخدم لتعريف نظام التشغيل وتزويده بعدد من المعلومات التي يحتاجها، مثل المسار الكامل لنظام التشغيل والمسار الذي توضع فيه الملفات المؤقتة وهكذا.



لتعرف أكثر عن التنسيقات الدقيقة لأنواع الملفات المختلفة، اتبع الرابط www.wotsit.org، ولمعرفة التطبيقات المرتبطة بلواحق الملفات، اتبع الرابط http://filext.com.

الملفات المحذوفة: ظاهرياً تتكون عملية حذف الملفات في نظام التشغيل Windows من خطوتين، الأولى هي وضع الملف في سلة المحذوفات والثانية إفراغها. يمكنك قبل أن تفرغ سلة المحذوفات أن تسترجع الملف إلى موقعه الأصلي باختيار الملف الموجود في سلة المحذوفات واستخدام أمر الاستعادة. لكن السؤال هو. ماذا يحصل للملف بعد إفراغ سلة المحذوفات؟

إذا عملت مع الحواسب لفترة ليست بالقصيرة، لا بد أنك تعلم أنه عندما تحذف ملفاً ما، فإنه لا يختفي فعلياً من على سطح القرص الصلب، حيث يستبدل نظام التشغيل Windows المحرف الأول لقيد الدليل للملف المحذوف بالمحرف سيغما (في النظام الست عشري E5)، مشيراً إلى أنه يجب أن لا يتم عرض الملف في قوائم الدليل، كما يتم تغيير قيود جدول تخصيص الملفات، وتعيين قيود الملفات المحذوفة إلى الصفر، وهذا يخبر نظام الملفات أنه يمكن استخدام المساحة التي كان يشغلها الملف. يستطيع ملف جديد، ملف منسوخ، أو ملف يزداد حجمه أن يستبدل الموقع حيث كانت تتوضع بيانات الملف المحذوف.

من الممكن فحص قطاعات القرص الصلب باستخدام محرر النظام الست عشري (برنامج يظهر البيانات الست عشرية التي تكوّن الملف)، وإعادة بناء الملف المحذوف يدوياً اعتماداً على معلومات القطاع. لكن هذا عمل متعب لأن الملفات عادة لا تحتل مساحات متجاورة من القرص ويمكن أن تتبعثر في جميع أنحاء القرص الصلب، لذلك من الأسهل بكثير استخدام برنامج مؤتمت لاسترداد الملفات المحذوفة.

تزداد فرصة استرداد ملف محذوف حديثاً من ملف آخر تم حذفه منذ ستة أشهر، لأنه من المحتمل مع مرور الوقت أنه تم الكتابة فوق المساحة من قبل بيانات من ملفات أخرى.

من الواضح أن الملفات المحذوفة هي مصدر ممتاز للحصول على دليل، وعليك دائماً القيام بما يلي:

- التحقق من سلة المحذوفات لمعرفة محتوياتها.
- استخدام برنامج لاسترداد الملفات، مثل البرامج التي سنعرضها في فقرة "أدوات تجميع الدليل" من هذا الفصل لتعرف إذا كان بإمكانك استعادة أية ملفات محذوفة. حتى لو لم تستطع أن تسترد الملف بأكمله لا يزال بإمكانك إنقاذ قطعاً متفرقة من الملف والتي قد تتضمن الدليل المطلوب.

ملفات مدير مهام الطباعة: يستخدم نظام التشغيل Windows إدارة مهام الطباعة عند طباعة مستند ما، وهذا يعني طباعة المستند في الخلفية وفي نفس الوقت يستطيع المستخدم متابعة عمله على المستند أثناء الطباعة.

تعمل عملية إدارة مهام الطباعة بالاعتماد على الملفات المؤقتة التي تتضمن البيانات المطلوب طباعتها بالإضافة إلى المعلومات المطلوبة لإنهاء عملية الطباعة، هناك نوعان لمهام الطباعة: EMF وRAW.

- **EMF**. وهو اختصار إلى Enhanced Metafile أي ملف فائق محسن، وهو النوع الافتراضي لمدير مهام الطباعة في النظام Windows، يتم تغيير المستند إلى تنسيق الملف الفائق قبل أن تتم طباعته.
- **RAW**. وهو نوع مدير مهام الطباعة المستخدم من قبل تطبيقات تعمل على أنظمة تشغيل أخرى غير النظام Windows. وهو يشير إلى أن البيانات جاهزة للطباعة ولن يتم تحويلها إلى نوع الملف الفائق.

يتم إنشاء ملفات إضافية ذات اللواحق SPL. وSHD.، لكلا التنسيقين EMF وRAW، لكل مهمة طباعة. تتضمن ملفات الظل SHD. ("shadow") معلومات حول مهمة الطباعة، أما ملفات SPL. تتضمن إما البيانات المطلوب طباعتها أو أسماء ملفات البيانات المطلوب طباعتها. تسمى هذه الملفات عادة باسم نوع مدير مهام الطباعة واللاحقة TMP.، مثلاً EMFxxxxxx.TMP~، وتحذف جميع الملفات ذات اللواحق SHD.، SPL.، وTMP. بعد الانتهاء من مهمة الطباعة.

يمكن أن تشكل ملفات مدير مهام الطباعة المحذوفة دليلاً هاماً. مثلاً، قد يدّعي المستخدم بأنه لم يطبع مستنداً تم إيجاده على القرص الصلب، لكن يمكن إثبات العكس باستعادة الملف الفائق للطباعة. ويمكن أن يكون قد تم مسح الملف قبل حذفه، لكن يمكن أن يتواجد الملف الفائق على القرص الصلب منذ وقت الطباعة.

يمكنك الحصول على مزيد من المعلومات عن مدير مهام الطباعة من موقع شركة Microsoft عن طريق البحث عن EMF وRAW، www.microsoft.com/technet.

الملفات المؤقتة لبرنامج تفحص الأقراص: عندما تنتهي جلسة النظام Windows بشكل خاطئ، مثلاً عند فصل التغذية عن الحاسب بدلاً من القيام بعملية إيقاف التشغيل، يعمل برنامج تفحص الأقراص عند بدء التشغيل لضمان عدم تلف نظام الملفات، ويمكن أن ينشئ البرنامج ملفات مؤقتة ذات اللاحقة CHK. في الدليل الجذر. لا يحذف البرنامج الملفات المؤقتة عند الانتهاء من العمل، وبالتالي يجب فحص أي ملف مؤقت له اللاحقة CHK. لأنه قد يحتوي أجزاء من الدليل الذي نتج من بعض الملفات الأخرى.

دفق البيانات البديل: يمكنك ربط بيانات إضافية لملف أو مجلد ضمن نظام الملفات NTFS لأنظمة التشغيل Windows NT/2000/XP، وهـــذا ما يسمى بدفق البيـــانات البـــديل ADS (Alternate Data Stream). يستطيع دفق البيانات البديل ADS إخفاء نص أو حتى ملف تنفيذي دون أن يكشف من قبل مستكشف Windows أو الأمر dir للنظام DOS. لا يمكن حذف البيانات المخفية ضمن ADS ما لم يتم حذف الملف أو الدليل الأب.

لا يعلم معظم المستخدمين ورجال شرطة الحواسب حول تدفقات البيانات البديلة ADSs، كما تزوّد هذه الميزة طريقة خفية لإخفاء المعلومات. اتبع الخطوات التالية لتتأكد بنفسك:

1. أنشئ ملف نصي ضمن الدليل الجذر باستخدام برنامج المفكرة وسمه test.txt، أدخل بعض النص ثم احفظ الملف.
2. تحقق من حجم الملف ضمن مستكشف Windows.
3. شغّل مربع حوار التشغيل، واطبع ما يلي: notepad test.txt:alternate.txt. يسألك برنامج المفكرة إذا كنت ترغب بإنشاء الملف، أجب بنعم. أدخل بعض النص ثم احفظ الملف.
4. الآن حاول إيجاد الملف alternate.txt، لا يظهر الملف ضمن أي دليل، لن تجد تطابق عند البحث اعتماداً على النص المدخل، كما يظهر برنامج التحرير الست عشري للملف test.txt النص المدخل ضمنه فقط حتى حجم الملف يبقى نفسه بالرغم من إضافة بيانات جديدة للملف. شيء ظريف أليس كذلك!
5. لتتأكد من وجود الملف alternate.txt أدخل العبارة التالية ضمن مربع حوار التشغيل: notepad test.txt:alternate.txt، والآن يمكنك الوصول إلى دفق البيانات البديل ADS.

إذا كان المشتبه به مستخدم حواسب محترف ويستخدم نظام الملفات NTFS ضمن أحد أنظمة التشغيل Windows NT/2000/XP، يجب أن تتحقق من وجود تدفقات البيانات البديل ADSs. يتوفر برنامج خدمي تابع للأمن الحاسم، والذي يكشف تدفقات البيانات البديلة على الرابط التالي www.crucialsecurity.com.

أساليب: سلة المحذوفات

إن فهم كيفية عمل سلة المحذوفات هو أمر هام جداً للمحقق.

سلة المحذوفات في الواقع هي مجلد نظام مخفي يسمى Recycled في أنظمة التشغيل Windows 9x/ME و Recycler في أنظمة التشغيل Windows NT/2000/XP. عندما يضع المستخدم

ملفاً ما ضمن سلة المحذوفات، يحذف نظام التشغيل Windows قيد الملف من المجلد الذي كان يتوضع ضمنه وينشئ قيداً لملف جديد ضمن المجلد Recycled، كما يضيف معلومات عن الملف إلى ملف مخفي اسمه INFO أو INFO2. أما بالنسبة للأنظمة Windows NT/2000/XP فيتم إنشاء مجلد فرعي مع معرّف أمن (SID) Security Identifier للحساب المسجل حالياً ضمن النظام.

تتضمن المعلومات المخزنة في الملف INFO ما يلي:

- اسم الملف الذي تم حذفه.
- تاريخ ووقت وضع الملف ضمن المجلد Recycled.
- موقع الملف السابق.

يمكن أن تكون هذه المعلومات هامة جداً لعملية جمع الدليل لأنها تثبت حذف الملفات من قبل المستخدم (لا يستخدم نظام التشغيل والتطبيقات سلة المحذوفات لحذف الملفات)، متى تم حذف الملفات، ومكان توضع الملفات سابقاً قبل حذفها.

يحذف الملف INFO في كل مرة يتم فيها إفراغ سلة المحذوفات، لكن يمكن استعادة هذا الملف مثل أي ملف آخر باستخدام برنامج لاستعادة الملفات.

اقرأ المقالة التعريفية رقم 136517 لشركة Microsoft لمزيد من المعلومات عن حذف الملفات ضمن Windows، على الرابط التالي:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;136517.

المساحة المهملة Slack Space

يعمل نظام التشغيل على قطع من البيانات ذات حجم ثابت تسمى التجمعات Clusters. التجمعات هي وحدات ذات حجم أصغري يستطيع نظام التشغيل Windows أن يخزن البيانات داخلها، يتكون الملف من متتالية من التجمعات. إذا كان الملف أو جزء منه يحتل تجمع ما بحجم أصغر من حجم التجمع، يحجز التجمع بكامله للملف. تسمى المساحة غير المستخدمة بين مكان انتهاء بيانات الملف ونهاية التجمع الذي تحتله "بالمساحة المهملة Slack Space". كمثال، استخدمت أنظمة التشغيل DOS و الإصدارات الأقدم من أنظمة Windows جدول تخصيص الملفات ذا الحجم 16 بت والذي كان يملك تجمعات ذات حجم كبير جداً، حيث كان حجم التجمع، بالنسبة لقرص صلب حجمه 2GB، هو 32KB. مثلاً إذا كان حجم ملف نصي هو 10KB فقط، يتم حجز كامل التجمع بحجم 32KB للملف، أي هناك حجماً قدره 22KB يمثل المساحة المهملة المرتبطة بالملف. الإصدارات الحالية من نظام التشغيل Windows أكثر فعالية وتملك تجمعات ذات حجم أقل بكثير.

المساحة المهملة قيمة للمحقق لأنها قد تتضمن أجزاءً من ملفات كبيرة محذوفة والتي تم إعادة حجز تجمعاتها وكتبت أجزاء منها بالبيانات الجديدة (يصرح بعض خبراء الفحص الشرعي للحواسب أن نسبة 25% من القرص الصلب هي عبارة عن مساحات مهملة). توجد أدوات تقوم بتجميع المساحات المهملة مع بعضها على القرص الصلب وتنشئ ملفاً كبيراً وحيداً والذي يمكن أن يُستعرض و يتم البحث ضمنه.

المساحة غير المخصصة Unallocated Space

المساحة غير المخصصة على القرص الصلب أو وسائط التخزين الأخرى هي تجمعات Clusters لا تستخدم حالياً من قبل أي ملف. لم تكتب أي بيانات إلى هذه المساحة أو تتضمن بيانات من ملفات محذوفة. مثل المساحة المهملة يمكن أن تزود المساحة غير المخصصة دليلاً قيماً للمحققين. تتوفر برامج خدمية للفحوصات الشرعية والتي تقوم بتجميع أي بيانات ذات النمط ASCII الموجودة ضمن المساحة غير المخصصة وكتابة البيانات التي قد تحوي الدليل إلى ملف وحيد ليتم فحصه.

ملف الترحيل في النظام Windows

تستخدم جميع إصدارات Windows ملف الترحيل Swap File (يسمى أيضاً ملف الصفحة Page File). يتوضع ملف الترحيل على القرص الصلب ويشكل جزءً من نظام إدارة الذاكرة في نظام التشغيل، حيث يتم ترحيل البيانات من وإلى ذاكرة الوصول العشوائي (Random Access Memory) إلى ملف الترحيل حسب الحاجة.

لنفترض أنك تستخدم برنامج Outlook لاستعراض بريدك الإلكتروني وتتصفح الإنترنت وتعمل على برنامج النصوص Microsoft Word لكتابة طلب عمل في نفس الوقت. هناك فرصة كبيرة أن تصفى بعض البيانات من بريدك الإلكتروني، من المواقع التي تتصفحها، وطلب العمل إلى ملف الترحيل، هذا يعني أن جميع أنواع الدليل بما فيها كلمات المرور، أرقام بطاقات الاعتماد، والبيانات الشخصية الأخرى يمكن أن تتوضع ضمن ملف الترحيل.

يسمى ملف الترحيل، اعتماداً على إصدار نظام التشغيل الذي تستخدمه:

- Win386.swp لأنظمة Windows 9x/ME
- Pagefile.sys للأنظمة Windows NT/2000/XP

تستخدم ملفات الترحيل بشكل مستمر من قبل نظام التشغيل، ويمكن أن يتراوح حجمها من عشرات إلى مئات الميغا بايتات. إذا أردت معرفة محتويات ملف الترحيل، يجب أن تقلع الحاسب باستخدام نظام تشغيل آخر غير النظام Windows (DOS، أو Linux)، ومن ثم تستخدم برنامج خدمي لاستعراض محتوياته.

يستخدم معظم رجال شرطة الحواسب برنامجاً خدمياً للبحث ضمن السلاسل الحرفية في ملف الترحيل، وذلك للبحث عن الدليل الذي يمكن أن يرتبط بالقضية، مثلاً، أسماء معروفة لملفات الصور المرتبطة بقائمة مصطلحات مرتبطة بالمخدرات. لكنك قد تضطر في بعض الحالات أن تتصفح الملف كاملاً يدوياً، لتبحث عن جزء مخفي من الدليل وقد ينتج عن هذا انقطاع القضية.

تجدر الملاحظة أنه مع أسعار الذواكر المعقولة، يستطيع المستخدم أن يركب ذاكرة كافية ضمن حاسبه وإلغاء عملية الترحيل دون التأثير على أداء الحاسب. كما يستطيع مستخدم ذكي أن يحذف ملف الترحيل قبل أن يستخدم نظام التشغيل Windows مجدداً (لا يمكن حذف ملف الترحيل أثناء عمل نظام التشغيل Windows).

تسجيل النظام Windows (Windows Registry)

يشكل التسجيل منجم ذهب لمن يبحث عن دليل على حاسب يعمل على نظام التشغيل Windows. يتضمن التسجيل كلمات المرور، قوائم بالملفات المستخدمة مؤخراً، أدلة لتطبيقات منصبة سابقاً، وجميع أنواع المعلومات القيمة. لا يملك معظم المستخدمين أدنى فكرة عن ماهية تسجيل النظام أو ماذا يتضمن. قبل أن نشرح كيفية استغلال تسجيل النظام، من الهام معرفة ما هو تسجيل النظام ومبدأ عمله.



لمعلومات مفصلة عن تسجيل النظام Windows اتبع الرابط:
www.regedit.com.

نبدأ بالنظام Windows 95، بدأت شركة Microsoft باستخدام ملفات قواعد بيانات تسمى مع بعضها بالتسجيل Registry لتخزين نظام التشغيل وبيانات التطبيقات. كانت قبل ذلك الوقت تخزن إعدادات النظام والتطبيقات ضمن ملفات نصية ذات اللاحقة INI.، لقد افتقرت تقنية التخزين البسيطة هذه إلى الكفاءة والأداء، والتي حسنها تسجيل النظام إلى:

- تم تخزين التسجيل، في الأنظمة Windows 9x/ME ضمن ملفين مخفيين في دليل Windows، يسميان USER.DAT و SYSTEM.DAT.

- تم تخزين التسجيل، في الأنظمة Windows NT/2000/XP ضمن عدة ملفات (من بينها NTUSER.DAT وUSRCLASS.DAT) متوضعة في المجلدات التالية \windows\system32\config و\Documents and Settings\{username}.

تسجيل النظام له بنية هرمية، ويسمى كل فرع "المفتاح key"، يمكن أن يحوي كل مفتاح مفاتيح أخرى بالإضافة إلى "القيم values". تتضمن القيمة البيانات الفعلية المخزنة ضمن التسجيل، ويمكن أن تكون القيم ذات نوع بيانات حرفي، منطقي، أو DWORD.

توجد خمسة فروع رئيسة ضمن تسجيل النظام (ستة في الأنظمة Windows 9x/ME)، ويتضمن كل فرع من الفروع نمطاً محدداً من البيانات. تتضمن الفروع ما يلي:

- **HKEY_CLASSES_ROOT**. أنواع الملفات ومعلومات ربط وتضمين الكائنات OLE لتطبيقات OLE.
- **HKEY_CURRENT_USER**. تشير إلى جزء من HKEY_USERS المرتبط بالمستخدم الحالي.
- **HKEY_LOCAL_MACHINE**. معلومات عن كل الأجهزة والبرمجيات على الحاسب. يخصص التكوين الحالي للأجهزة إلى الفرع HKEY_CURRENT_CONFIG.
- **HKEY_USERS**. تفضيلات لكل مستخدم للحاسب. يتضمن الفرع الافتراضي في الأنظمة Windows 9x/ME المستخدم الحالي. أما في الأنظمة Windows NT/2000/XP يتضمن الفرع قالباً للمستخدمين الذين تمت إضافتهم مؤخراً.
- **HKEY_CURRENT_CONFIG**. يشير إلى جزء من الفرع HKEY_LOCAL_MACHINE المرتبط بالتكوين الحالي للأجهزة الصلبة.
- **HKEY_DYN_DATA (في الأنظمة Windows 9x/ME فقط)**. تشير إلى معلومات ركب وشغل ضمن HKEY_LOCAL_MACHINE.

يصل نظام التشغيل والتطبيقات إلى التسجيل باستمرار باستخدام استدعاءات واجهة برمجة التطبيقات API (Application Programming Interface)، لقراءة البيانات، وكتابة بيانات جديدة للفروع والمفاتيح. يمكنك استعراض وتحرير تسجيل النظام باستخدام البرنامج الخدمي RegEdit، والذي له بنية شجرية مثل مستكشف Windows، كما هو موضح في الشكل 5-1، يمكنك الضغط على الفروع والمفاتيح لإظهار المعلومات.

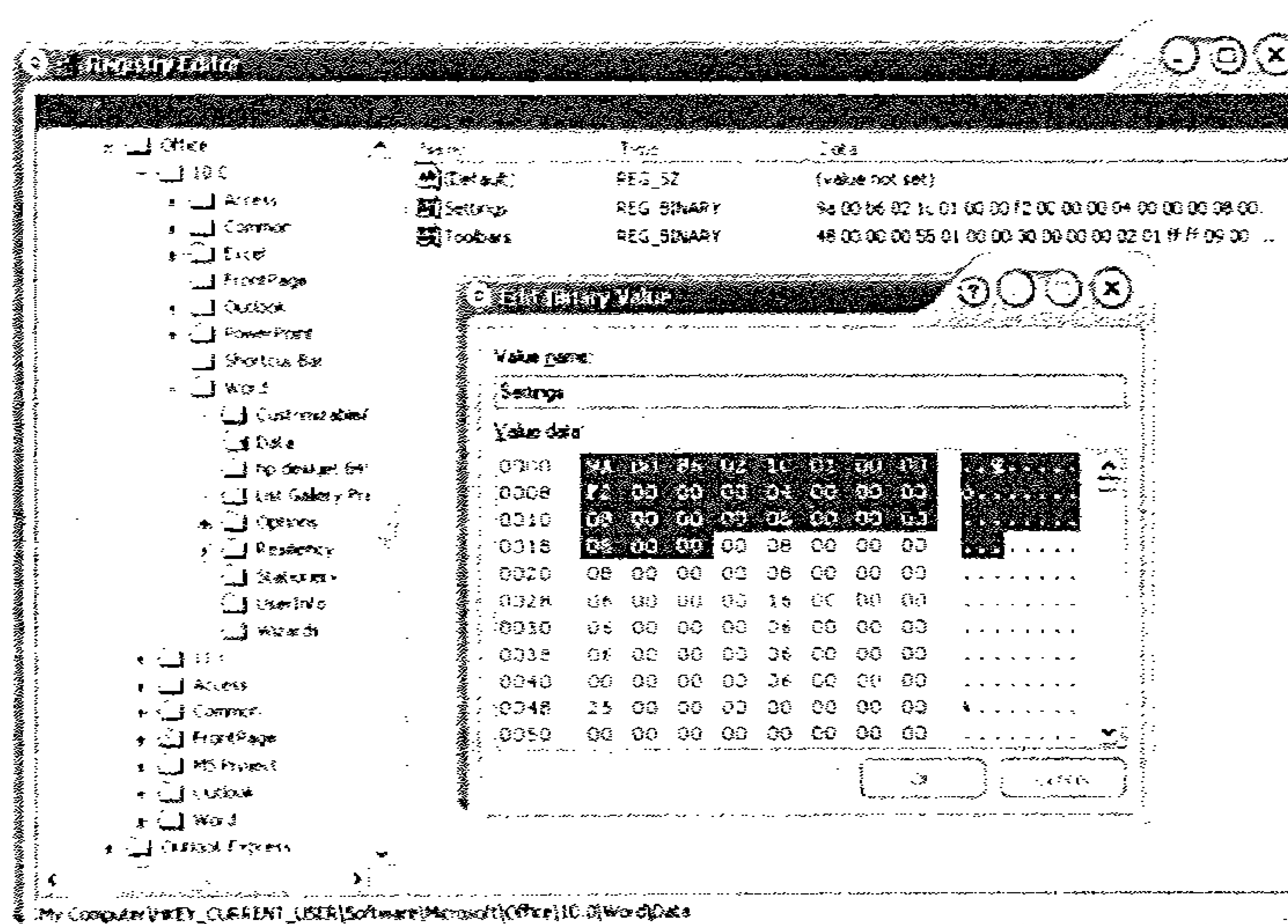


قد يؤدي تغيير قيم المفاتيح ضمن تسجيل النظام بدون أن تعرف ماذا تفعل، إلى إفساد نظام التشغيل والتطبيقات.

عندما تحذف قيم ومفاتيح التسجيل، يمكن مع ذلك أن تكون موجودة ضمن ملفات التسجيل الفعلية، مع أنها لا تظهر من خلال البرنامج الخدمي RegEdit. يمكن أن تكتشف دليلاً بصورة مفاجئة عند البحث من خلال هذه الملفات باستخدام برنامج تحرير ست عشري. الطريقة الوحيدة ليتأكد المستخدم من إزالة المفاتيح والقيم عند حذفها من خلال البرنامج RegEdit أو برامج أخرى، هي إعادة بناء وضغط تسجيل النظام.



بدلاً من استخدام البرنامج الخدمي RegEdit لتتحقق يدوياً من معلومات التسجيل، يمكنك تحميل نسخة مجانية من البرنامج الخدمي DumpReg التابع للشركة SomarSoft، لتفريغ التسجيل كاملاً وكأنه ملف نصي بسيط. يمكنك التحميل من خلال الرابط www.systemtools.com/somarsoft.



الشكل (5-1) تسجيل النظام المفتوح باستخدام البرنامج الخدمي RegEdit، ويعرض اسم مستند Word المستخدم مؤخراً ضمن مفتاح الإعدادات.

قوائم الملفات الأخيرة

تملك معظم التطبيقات قائمة بالملفات الأخيرة MRU (Most Recently Used)، تظهر هذه القائمة عادة في أسفل قائمة "ملف" والتي تحوي أسماء ومسارات الملفات التي تم فتحها مؤخراً

باستخدام هذا التطبيق. يمكن أن تكون هذه المعلومات قيمة بمعرفة ما هي الملفات التي كان يعمل عليها المستخدم. غالباً ما تخزن هذه المعلومات ضمن تسجيل النظام على شكل قيم.

الحافظة CLIPBOARD

إذا كان الحاسب لا يزال يعمل عندما تريد فحصه، تحقق من الحافظة عن أي معلومات يمكن أن تكون قد نسخت أو قصت مؤخراً، لكن محتويات الحافظة ليست دائمة وعند إيقاف تشغيل الحاسب لن تحتفظ الحافظة بالبيانات إلى المرة التالية التي يتم فيها تشغيل الحاسب. يوجد برنامج مستعرض للحافظة يأتي مع نظام التشغيل Windows والذي يعرض النصوص والصور الموجودة حالياً في الحافظة. ابحث ضمن القرص الصلب على الملف Clipbrd.exe وشغل المستعرض.

أخطاء المستعرض الصنعية

تترك مستعرضات الويب عدداً من الأشياء التي يمكن أن تستخدمها لمعرفة عادات أحدهم عند التجول عبر شبكة الإنترنت. يحتفظ المستعرض بكمية كبيرة من المعلومات ويجب أن يكون أحد الأماكن الأولى التي عليك التحقق منها عند البحث عن الأدلة.

الذاكرة المخبئية CACHE: تعني عملية التخزين المخبئي أنه يمكن بدلاً من تحميل صفحات الويب المتكررة والصور، أن يحتفظ المستعرض بنسخة محلية للمحتويات على القرص الصلب. يستمتع المستخدمون بهذا الأمر بسبب سرعة تحميل الصفحة، وأنت تستمتع كذلك الأمر لأنك تستطيع الوصول بسهولة إلى نسخة من محتوى الويب الذي قام المشتبه به باستعراضه.

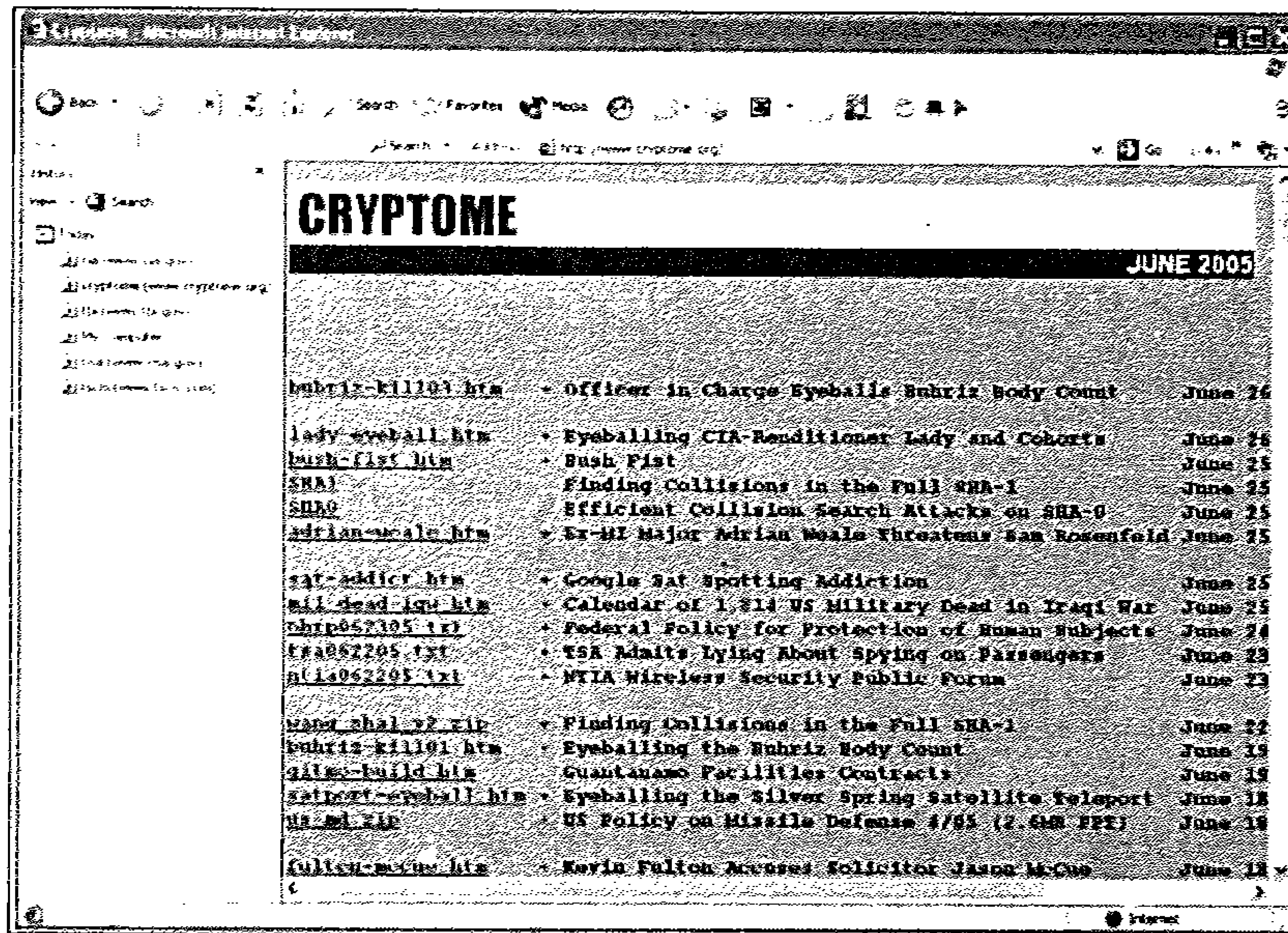
تعمل الذاكرة المخبئية للمستعرض على مبدأ الداخل أولاً، الخارج أولاً (first in – first out). تتم إضافة محتوى جديد إلى الذاكرة المخبئية باستمرار حتى تصل إلى حد معين، حيث تحذف البيانات الأقدم لتحرير المساحة لمحتوى الذاكرة المخبئية الأحدث. يتم تعيين معظم الذواكر المخبئية للمستعرضات إلى حجم كبير جداً وتخزن تاريخاً طويلاً جداً للملفات.

تخزن ملفات الذاكرة المخبئية، لبرنامج Internet Explorer، ضمن مجلد \Temporary Internet Files. الملفات ليست مضغوطة ويمكن إظهار محتواها باستخدام أي مستعرض ويب.

المفضلة FAVORITES: تزود مواقع الويب التي يزورها المشتبه بعض الإشارات والدلائل للجريمة التي تقوم بالتحقيق فيها. اضغط أيقونة المفضلة Favorites ضمن شريط الأدوات العلوي في برنامج مستعرض الإنترنت Internet Explorer، تظهر نافذة تحوي محددات لمواقع المعلومات URLs (Uniform Resource Locator) والتي تم اختيارها إلى المفضلة، ثم اضغط بزر الفأرة اليمين على محدد موقع معلومات واختر الأمر خصائص، تظهر نافذة تحوي معلومات حول زمن إدخال

الرابط إلى المفضلة بالإضافة إلى عدد مرات زيارة الصفحة (لا تعرض دائماً هذه المعلومات). يمكن عرض المفضلة بطريقة أخرى وهي فتح مجلد المفضلة.

المحفوظات HISTORY: تتضمن جميع المستعرضات ميزة تسمى المحفوظات والتي تستعرض مواقع الويب التي تم زيارتها خلال الأيام أو الأسابيع الفائتة. تفهرس المحفوظات تلقائياً جميع مواقع الويب التي يزورها المستخدم. اضغط أيقونة الساعة الشمسية التي تمثل المحفوظات ضمن شريط الأدوات في برنامج مستعرض الإنترنت، تظهر نافذة تحوي جميع محددات مواقع المعلومات التي تم زيارتها، كما هو مبين في الشكل 2-5. يمكننا أن نشير هنا إلى أن المحفوظات تقدم كماً كبيراً جداً من المعلومات عن نشاطات الإنترنت الخاصة بأحد ما.



الشكل (5-2) يمكن أن تقدم محفوظات المستعرض Internet Explorer معلومات قيمة عن عادات تصفح الإنترنت التي يقوم بها المشتبه به.

معلومات الإكمال التلقائي AUTOCOMPLETE INFORMATION: يحفظ مستعرض الإنترنت بشكل افتراضي كل شيء يطبعه المستخدم ضمن نموذج لصفحة ويب، قد تشمل هذه المعلومات أسماء الحسابات، كلمات المرور، العناوين، وجميع أنواع المعلومات الشخصية الأخرى، حيث تكون المعلومات موجودة ضمن النموذج عند زيارة المستخدم الثانية لنفس الصفحة، يكون هذا الأمر مناسباً للمستخدم كما أنه يكون مناسباً أيضاً للمحقق. يمكن الحصول على معلومات الإكمال التلقائي بفتح مواقع الويب المخزنة ضمن المحفوظات أو عن طريق فحص المفاتيح والقيم المرتبطة

بمستعرض الإنترنت ضمن تسجيل النظام. (تحقق من المواقع HKEY_CURRENT_USER، أو HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion ثم ابحث عن المفاتيح "Explorer" و"Internet Settings" أو انظر في المفاتيح الفرعية للفرع HKEY_CURRENT_USER أو HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer keys).

ملفات تعريف الارتباط Cookies: يمكننا أن نعرف ملفات تعريف الارتباط، بدون الدخول إلى التفاصيل، بأنها بيانات قليلة يخزنها ملقم الويب على الحاسب المحلي. لقد جرت مناقشة حامية حول ملفات تعريف الارتباط، في التسعينات عند انتشار استخدام شبكة الإنترنت، وإمكانية تعقب الشركات الاستخدام الشخصي للويب عن طريقها. لكن بالرغم من صحة هذا الأمر إلى حد ما، فقد تمت تهدئة الخلاف عندما أدرك الناس أن ملفات تعريف الارتباط لا تشكل تهديداً كبيراً للسرية (حتى لو لم تكن كذلك، قليل من الناس اهتموا بهذا). يتم استخدام ملفات تعريف الارتباط عادة من قبل ملقمات الويب، ولكن يمكنك استخدامها أيضاً لتكتشف عادات التصفح الخاصة بالمشتبه به لأنها تتضمن مرجعاً إلى موقع الويب الذي تمت زيارته، بالإضافة إلى معلومات عن تاريخ التعديل والوصول إلى الملفات.

الإعداد الافتراضي لمستعرض الويب هو استخدام ملفات تعريف الارتباط Cookies، يمكن فتح هذه الملفات من مجلد Cookies\ باستخدام أي برنامج نصوص.

مستخدمو البريد الإلكتروني E-MAIL CLIENTS

تشكل تطبيقات البريد الإلكتروني مصدراً هاماً للحصول على الدليل. إن البريد الإلكتروني حاضر في كل مكان من حولنا، مع تقدير إرسال حوالي 31 مليار رسالة إلكترونية يومياً عبر العالم. لا يفكر الكثير من المستخدمين عن محتويات رسائلهم التي يرسلونها ويستقبلونها، بالرغم من إمكانية حصول المحقق على معلومات مباشرة أو غير مباشرة عن نشاطاتهم.

الخطوة الأولى لاستخدام البريد الإلكتروني كدليل هي التعرف على تطبيق البريد الإلكتروني الخاص بالمستخدم، حيث عليك معرفة كيفية عمل التطبيق، الميزات التي يقدمها، والأوامر الكثيرة الاستخدام. تأكد من حصولك على فهم تام لتطبيق البريد الإلكتروني قبل أن تبدأ باستخدامه للحصول على الدليل. الأمر الجيد هو بالرغم من وجود الكثير من تطبيقات البريد الإلكتروني، يتم استخدام عدداً قليلاً منها فقط وتتضمن التطبيقات التالية Microsoft Outlook، Outlook Express، AOL Mail، Eudora، Pegasus، وNetscape Communicator.

بغض النظر عن البرنامج التي تتفحصه، فإن إحدى نقاط الضعف الأساسية لمعظم تطبيقات البريد الإلكتروني هي تطبيق الحماية باستخدام كلمة المرور على عملية تسجيل الدخول فقط، حيث

تفتقد معظم هذه التطبيقات للميزات الأمنية والتي يجب أن تمنع استعراض الرسائل التي تم تحميلها، حذفها مؤقتاً، أو إرسالها (إذا تم الاحتفاظ بنسخ منها) مسبقاً، في حال كنت تملك الوصول الفيزيائي للحاسب.

أمر آخر يشكل خطراً للمستخدم هو وجود خيار في معظم تطبيقات البريد الإلكتروني لحفظ اسم الحساب وكلمة المرور، أي لن يتم إدخال هذه المعلومات في كل مرة. لكن بالرغم من أن هذا الخيار ملائم للمستخدم إلا أنه يشكل خطراً كبيراً جداً لأن أي شخص يتمكن من الوصول الفيزيائي إلى الحاسب سيتمكن من إرسال واستقبال الرسائل الإلكترونية.

يجب أن تراعي خمسة أماكن عند بحثك عن دليل مرتبط بالبريد الإلكتروني وهي:

- **البريد الوارد Inbox**. يتضمن البريد الوارد جميع الرسائل الإلكترونية التي استلمها المشتبه به، لذلك هو المكان الأول الذي يجب أن تتفقده عند بحثك عن الدليل، وعليك أن تستعرض الترويسات الكاملة للرسائل لأنه قد تكتشف معلومات مرتبطة بأصل الرسالة.
- **الرسائل المرسلة Sent Messages**. تتضمن الكثير من تطبيقات البريد الإلكتروني خياراً للاحتفاظ بنسخة من الرسائل المرسلة، وهذا أمر هام لأنه إذا كان هذا الخيار مفعّلاً، يمكنك استعراض جميع الرسائل الإلكترونية التي أرسلها المشتبه به.
- **الملفات المرفقة المخزنة Saved Attachments**. حالما يرسل المستخدم ملفاً مرفقاً، يحوّل التطبيق نسخة من الملف المرفق إلى تنسيق يمكن إرساله عبر الإنترنت، نموذجياً ملحقات بريد الإنترنت متعدد الأغراض MIME[1]. تحذف الملفات المحولة تلقائياً بعد إرسال الرسالة بنجاح. إذا تمكنت من استرجاع هذه الملفات المحذوفة، يمكن إعادة تحويلها من التنسيق MIME إلى تنسيقها الأصلي باستخدام البرنامج الخدمي Munpack.exe (أدخل الكلمة munpack ضمن محرك بحث لإيجاد مواقع لتحميل هذا البرنامج). كما يمكنك تصفح المجلدات المؤقتة بحثاً عن الملفات المرفقة.
- **مجلد المسودة Drafts ومجلد الرسائل المعلقة Pending**. مكان آخر للبحث عن الدليل هو مجلد المسودة ومجلد الرسائل المعلقة، والتي تتضمن الرسائل الإلكترونية التي لم يتم إرسالها بعد.
- **الرسائل المحذوفة Deleted Messages**. تستخدم معظم تطبيقات البريد الإلكتروني طريقة سلة المحذوفات لحذف الرسائل، حيث يتم الاحتفاظ بالرسالة ضمن مجلد أو مكان تخزين

[1] MIME اختصار للعبارة Multipurpose Internet Mail Extensions، وهو معيار يعمل على توسيع بروتوكول نقل البريد البسيط SMTP ليجعله قادراً على نقل بيانات لا نصية مثل الأصوات والصور والملفات الثنائية بشكل عام وذلك دون الحاجة لتحويلها إلى محارف ASCII أولاً.

منفصل حتى يقوم المستخدم بإفراغ السلة أو يتخلص من الرسالة الإلكترونية المحذوفة، وحتى ذلك الوقت يمكنك أن تستعرض هذه الرسائل.

أساليب: الملفات ذات اللاحقة DAT

ينشئ مستعرض الإنترنت ملفاً مخفياً اسمه index.dat ضمن المجلدات التالية cache، cookies، و history، ويحوي هذا الملف معلومات الفهرسة الخاصة بمستعرض الإنترنت كما يحوي أيضاً تفصيلاً كاملاً عن نشاطات تصفح الإنترنت من قبل المستخدم. ينسخ الملف index.dat إلى ثلاثة مجلدات:

- **المجلد Cache:** يتضمن الملف index.dat الموجود ضمن المجلد Temporary Internet Files\، أسماء محددات مواقع الملفات URLs، علامات التاريخ والوقت، ومؤشرات إلى المجلد Cache المنتشرة بين عدة مجلدات فرعية اسمها Cache.
- **المجلد Cookie:** يتضمن الملف index.dat الموجود ضمن المجلد Cookies\ أسماء محددات مواقع الملفات URLs، علامات التاريخ والوقت، ومؤشرات إلى ملفات تعريف الارتباط Cookies المخزنة ضمن مجلد Cookie.
- **المجلد History:** يخزن الملف index.dat ضمن مجلد المحفوظات History محددات مواقع الملفات التي تمت زيارتها بالإضافة إلى علامات التاريخ والوقت. يستخدم مستعرض الإنترنت هذه البيانات لعملية الإكمال التلقائي ولتحديد فيما إذا تم زيارة الروابط المعروضة ضمن الصفحة الحالية.

يختلف موقع هذه المجلدات باختلاف إصدار نظام التشغيل:

- في الأنظمة Windows 9x/ME: \WINDOWS\
- في الأنظمة Windows 9x/ME ذات التشكيلات الجانبية الخاصة بمستخدم معين: \WINDOWS\PROFILES\user_name
- في الأنظمة Windows NT/2000/XP:

\DOCUMENTS AND SETTINGS\user_name\LOCAL SETTINGS

مع أن الملفات index.dat ليست نصية، لكن يمكن فتحها باستخدام برنامج الدفتر WordPad أو أي محرر نصوص آخر لاستعراض جزء من البيانات. يوجد أيضاً أدوات أخرى يمكن استخدامها مثل index.dat Viewer والذي يستعرض محتويات الملف، يمكنك تحميل هذه الأداة من الرابط التالي www.exits.ro/index-dat-viewer.html.

المراسلة الفورية Instant Messaging

لقد ازدادت شعبية المراسلة الفورية IM، سواء عن طريق خدمة المحادثة عبر الإنترنت Internet Relay Chat (IRC) أو الخدمة الخاصة America Online باستخدام إصدارات Yahoo أو Microsoft، بشكل كبير خلال السنوات الماضية. إذا تم تثبيت برنامج للمراسلة الفورية على القرص الصلب فيمكن أن تجد معلومات قيمة عن طريقه، فقد تحصل على الدليل من خلال قوائم الأصدقاء، أسماء الحسابات للأشخاص الذين أرسلوا رسائل مؤخراً، وسجلات الرسائل المخزنة.



إذا حصلت على كلمة المرور الخاصة بحساب برنامج المراسلة الفورية، وهذا أمر ليس بالصعب إذا قمت باستخدام الأدوات التي سنعرضها في الفصل السابع، فإنك تستطيع جمع الأدلة من خلال التنكر بشخصية المشتبه به وإجراء محادثات مع الأشخاص من قائمة الأصدقاء.

مضبوط: رجال الشرطة ضد James Kopp

تم القبض على James Kopp، الذي اتهم بقتل الطبيب Barnett A. Slepian في الثالث والعشرين من شهر تشرين الأول (أكتوبر) عام 1998، في شهر نيسان (أبريل) عام 2001 في فرنسا. James Kopp هو ناشط ضد قانون الإجهاض، حيث قام Kopp بإطلاق النار وقتل الطبيب Slepian في منزله باستخدام بندقية روسية.

سعى مكتب التحقيقات الفدرالي إلى القبض على Kopp بأي طريقة، وقاموا بإضافته إلى "لائحة العشرة الأوائل المطلوبين".

استطاع Kopp مغادرة الولايات المتحدة وجعل قوى القانون تقوم بمطاردته عبر أوروبا قبل القبض عليه، وأثناء عملية الملاحقة اعتقل المكتب شريكين مزعومين للمتهم وهما Loretta Marra و Dennis Malvasi من Brooklyn في مدينة New York. لقد تم اتهام هؤلاء بعد أن قام مكتب التحقيقات الفدرالي بالاستماع إلى مخابراتهم الهاتفية خفية، وتثبيت أجهزة تنصت في شقتهم، ومراقبة بريدهم الإلكتروني.

لقد كان من الواضح أن كلاً من Kopp و Marra استخدموا نظام بريد إلكتروني معتمد على شبكة الويب للاتصال فيما بينهم، وبدلاً من تبادل الرسائل الإلكترونية استخدموا الحساب نفسه، وكانوا يخزنون الرسائل ضمن مجلد المسودات. من الجلي أن كلاً منهما كان يتمتع بحس أمني عالي وأدركوا أن إرسال الرسائل الإلكترونية عبر الإنترنت يمكن أن يكشف ويتم تعقبه واعتقدوا أن بإمكانهم التخلص من هذا التهديد بعدم إرسال الرسائل على الإطلاق. لكن الأمر الذي لم يفكروا به هو أن عناوين IP للحواسب التي استخدموها للوصول إلى بريد الويب

الإلكتروني يتم تسجيلها بصورة دورية. كما يتعاون المزودون لخدمة البريد الإلكتروني المعتمدة على الويب مع قوى القانون بصورة دورية أيضاً. وقد صرح مكتب التحقيقات الفدرالي أنه استخدم أمر موافقة لاستخدام لوائح الأرقام المطلوبة وأجهزة التعقب لتطبيقها على البريد الإلكتروني بالتعاون مع التحقيقات. من المحتمل أن السجلات كانت من موقع البريد الإلكتروني ودلت إلى مقهى إنترنت في فرنسا، حيث اتخذت قوى المراقبة الفيزيائية مواقعها ومن ثم ترصدت Kopp وألقت القبض عليه.

تمت إدانة Kopp بتهمة القتل المتعمد في شهر آذار (مارس) عام 2003، وأعلن المدعون أنهم سيسعون بعقوبة تتراوح من 25 عاماً في السجن إلى الحكم المؤبد، وذلك عند إصدار حكمه.

الأقراص الصلبة HARD DRIVES

قد تواجه في بعض الأحيان قرصاً صلباً لا تستطيع الوصول إليه خلال عملية التحقيق، فقد يكون قد تعرض القرص الصلب للانهيار، أو تضرر نتيجة نيران أو مياه، أو تم إعادة تهيئته لمحاولة القضاء على دليل محتمل. لكن حتى في هذه الظروف الشديدة، فمن الممكن استرجاع الدليل من القرص.

توجد طريقتا ترميم لاسترداد البيانات من القرص الصلب: برمجيات الاسترداد وخدمات الاسترداد التجارية.

- **برمجيات الاسترداد.** قد تستطيع تطبيقات استرداد البيانات إحياء القرص الصلب، إذا لم يتعرض لضرر فيزيائي. تسترد هذه البرامج الخدمية الأقسام المحذوفة، تعيد المحركات المنطقية، وتحدد وتسترد الملفات والمجلدات المحذوفة. انظر ضمن فقرة "أدوات جمع الأدلة" لاحقاً في هذا الفصل للحصول على أمثلة لعدة تطبيقات استرداد.
- **خدمات الاسترداد التجارية.** الخيار الثاني أمامك هو إرسال القرص الصلب من جديد إلى شركة متخصصة باسترداد البيانات. توظف هذه الشركات خبراء تقنيين يقومون بتحليل القرص الصلب إلى أجزاءه الأولية في غرف نظيفة واستخلاص البيانات باستخدام تجهيزات وبرمجيات خاصة، بدلاً من مجرد استخدام برمجيات الاسترداد التجارية. وفي حال تضرر طبقة التخزين للقرص الصلب فيزيائياً، يبقى احتمال استرداد بعض البيانات وارداً. تستخلص الشركات البيانات الأصلية وتخزن الملفات المستردة على أقراص DVD، أقراص مضغوطة، أو أشرطة مغناطيسية. خدمات هذه الشركات ليست بالرخيصة، ويمكن أن تدفع ما بين 500$ إلى 1500$ مقابل استرداد ناجح لإخفاق القرص الصلب (وبالتأكيد المحاولات الفاشلة أرخص بكثير).



يمكنك استعراض لائحة شاملة لأعمال استرداد البيانات الأوروبية والأمريكية على الرابط www.datarecoverylinks.com. من أحد أكبر وأشهر الشركات التي تتلقى كثيراً من طلبات المؤسسات التجارية وقوى القانون وهي الشركة Ontrack Data International (أحد قادة استرداد البيانات، المكتسبة من تكتل الشركات Kroll في شهر حزيران عام 2002 – لمزيد من المعلومات اتبع الرابط www.ontrack.com) والشركة DriveSavers Data Recovery (تأسست هذه الشركة عام 1985، تستطيع الشركة إخراج البيانات من 24 إلى 48 ساعة – لتفاصيل أخرى اتبع الرابط www.drivesavers.com).

الأقراص المرنة FLOPPY DISKS

الأقراص المرنة هي وسائط تخزين قديمة الطراز، بسبب سعتها التخزينية المحدودة. إلا أن القرص المرن يستمر في الوجود ومن الممكن أن يتم استخدامه في معظم التحقيقات الحاسبية. يمكن استخدام برمجيات استرداد الملفات وخدمات استرداد البيانات المحترفة للشركات المنفذة لاسترجاع بيانات القرص الصلب، للأقراص المرنة.

من الجدير ذكر النقطتين التاليتين فيما يخص الأقراص المرنة والتحقيقات:

- إذا استخدم المشتبه به طريقة مسح الملفات (الكتابة الفوقية للملفات التي تضم بيانات لضمان عدم استرداد محتوياتها بعد الحذف)، فقد لا ينجح في مسح الملفات من الأقراص المرنة مقابل نجاحه في هذا للأقراص الصلبة. مسارات البيانات في الأقراص المرنة واسعة جداً وآليات المحرك متساهلة جداً بما يخص محاذاة الرأس، حيث تتمكن بعض البرمجيات استرداد البيانات على أحد أوجه الموقع المستعمل.
- طور المختبر الشرعي للحاسب التابع لوزارة الدفاع DCFL (Department of Defense Computer Forensics Laboratory) في ولاية Maryland تقنيات لوصل الأقراص من أجل إعادة بناء الأقراص المرنة 3.5 أنش و5.25 أنش والتي تعرضت للقص، القطع، الالتواء، التمزيق، الإذابة، أو المنتزعة من محور القرص. وبعد إعادة تجميع الأقراص يمكن استرداد البيانات منها. يقدم المختبر وثيقة "خاصة بقوى القانون فقط" والتي تصف هذه العملية، يمكنك زيارة موقع المختبر على الإنترنت www.dcfl.gov.

الذاكرة MEMORY

إذا كان الحاسب لا يزال يعمل، فقد ترغب في استعراض محتويات ذاكرة الوصول العشوائي Random Access Memory (RAM) أو أن تنجز تفريغاً لذاكرة النظام الكاملة إلى القرص

لتفحصها لاحقاً. فقد تقيم كلمات المرور، المستندات، وأجزاء أخرى من الأدلة في الذاكرة ولا تكون موجودة ضمن القرص الصلب. (ملاحظة: حفظ الذاكرة على القرص الصلب ليس محبذاً لأنه يعدّل وسائط التخزين الأصلية).

أدوات جمع الأدلة

يتوفر عدد من الأدوات لمساعدتك على جمع وتحليل الدليل الرقمي، الكثير من هذه الأدوات عامة وتم تصميمها منذ البدء لإدارة النظام. كما توجد حفنة من البرامج الخدمية والتي تم بناؤها بشكل خاص لأعمال الاختبارات الشرعية، مع أن بعض أدوات الاختبارات الشرعية البسيطة والتي تعمل على سطر الأوامر مجانية، لكن البرمجيات التجارية الأخرى والمصممة بوضوح لتستخدم في التحقيقات تكون مكلفة جداً، هنا يمكننا القول أن الاختبارات الشرعية هي تجارة مناسبة ولكن بسبب تزايد الطلب على هذا النوع من الأدوات على مدى السنوات القادمة ومع زيادة المنافسة (وخاصة من قبل البرامج المجانية الصادرة من قبل مجتمع المصدر المفتوح)، فيمكن أن تظهر أدوات جديدة أقل تكلفة.



استمر Dan Mares في أعمال الاختبارات الشرعية لمدة طويلة ويقوم بإنتاج بعض الأدوات البرمجية الشائعة الاستخدام، كما يحافظ أيضاً على قائمة بالتجهيزات الصلبة والبرمجيات على الرابط:
www.maresware.com/maresware/linksto_forensic_tools.htm.

أدوات المضاعفة الشرعية

تم تصميم أدوات المضاعفة الشرعية لإنشاء صورة مرآة للقرص الصلب، حيث يتم تكوين نسخة مطابقة تماماً للقرص الصلب بتاً بتاً وذلك بدلاً من مجرد القيام بالنسخ العادي للملفات. يتم عادة وصل القرص الصلب الخاص بالمشتبه به وقرص صلب فارغ إلى الحاسب، ومن ثم يتم إقلاع الحاسب باستخدام أي نظام تشغيل ما عدا النظام Windows ويتم تشغيل برنامج المضاعفة. سوف نستعرض مجموعة من أدوات النسخ شائعة الاستخدام في الاختبارات الشرعية الحاسبية في الفقرات التالية.

الأداة SAFEBACK: وهي أداة مضاعفة تعمل على نظام التشغيل DOS والمعروفة منذ عام 1990. تقوم الأداة بالوصول مباشرة إلى الأقراص الصلبة IDE (إلكترونيات الأجهزة المتكاملة Integrated Device Electronics) وذلك دون التحقق من إعدادات محرك BIOS الهندسية، مضاعفة

قرص صلب إلى قرص صلب آخر، شريط، أو وسائط تخزين قابلة للإزالة، وإضافة معلومات المجموع التدقيقي إلى ملفات محرك الصورة والتي تضمن تكامل البيانات. تستخدم قوى القانون، الجيش، والوكالات الاستخباراتية البرنامج SafeBack بصورة واسعة، حتى أن البرنامج يملك رقماً خاصاً للمنتج وذلك لسهولة طلبه من قبل الحكومة. تبلغ قيمة البرنامج 595 دولار أمريكي، ولمعلومات أخرى عن البرنامج SafeBack، اتبع الرابط www.forensics-intl.com/safeback.html.

برنامج NORTON GHOST: تم تصميم هذا البرنامج بالأصل للمسؤولين عن النظام وذلك ليقوموا بنسخ احتياطية للأقراص الصلبة، ومن ثم أصبح هذا التطبيق معروفاً بسبب سهولة استخدامه، كلفته المنخفضة، تعددية الاستخدامات من قبل رجال شرطة الحواسب والفاحصين الشرعيين. تكلفة هذا البرنامج 69.95 دولار أمريكي، ولمزيد من المعلومات قم بزيارة موقع الشركة الخاصة بالبرنامج www.symantec.com.

برنامج LINUX DD: يشكل البرنامج الخدمي DD وهو اختصار للعبارة data dumper (مفرّغ البيانات) خياراً لنسخ الدليل، وذلك للأشخاص الذين لديهم معرفة بنظام التشغيل Linux أو للمحققين ذوي الميزانية المحدودة. يُستخدم برنامج dd بالأصل لنقل البيانات بين الملفات ويمكن استخدامه كذلك لمضاعفة الأقراص الصلبة، لكن المشكلة الأساسية لهذا البرنامج هي عدم سهولة واجهة استخدامه كما أن أوامره مبهمة وخاصة بالنسبة للشرطي الذي لديه خبرة بنظام التشغيل Windows فقط. مثلاً لتقوم بمضاعفة قرص صلب إلى نظام شريط احتياطي باستخدام البرنامج dd، عليك طباعة السطر التالي ضمن محرر الأوامر dd if=/dev/had of=/dev/rst0.



أصدرت وزارة الدفاع الأمريكية تقريراً خاصاً في شهر آب (أغسطس) عام 2002، حول استخدام برنامج dd في الاختبارات الشرعية الحاسبية. اتبع الرابط www.ncjrs.org/pdffiles1/nij/196352.pdf.

أدوات جمع الأدلة المؤتمتة

قد تشكل عملية تجميع وتحليل الدليل من قرص صلب أو أي وسط تخزين آخر عملية متعبة ومستهلكة للوقت. اعتمد أغلب المحققين على مجموعة من أدوات سطر الأوامر لفحص واستخلاص الدليل الحاسبي، ومنذ حوالي خمس سنوات أو أكثر فقط ظهرت أدوات لمعالجة وتجميع الدليل، القائمة بذاتها، سهلة الاستخدام، والمبنية على النظام Windows. لقد قلصت هذه التطبيقات بصورة كبيرة الزمن المطلوب لتجميع وتحليل الدليل وكذلك عدد المهارات التقنية التي يحتاجها الفاحص ليتمكن من إنجاز تحقيقات حاسبية فعالة. تتوفر حالياً ثلاث أدوات شرعية تضم عدداً من الميزات ضمن حزمة برمجية واحدة.

أدوات ENCASE: يعتبر EnCase من أشهر أدوات الاختبارات الشرعية القائمة بذاتها وأكثرها استخداماً في الأسواق اليوم (حالياً، يستخدم هذا المنتج من قبل أكثر من ألفي وكالة قانون عبر العالم). وبما أن EnCase من أشهر الأدوات حالياً لذلك سوف نشرحه بالتفصيل.

من وجهة نظر التجهيزات الصلبة، يعمل EnCase على أحدث الحواسب الشخصية ذات الأنظمة Windows 9x/ME أو Windows NT/2000/XP. يحتاج برنامج EnCase مفتاح حماية dongle يوصل إلى منفذ USB أو منفذ تفرعي وذلك من أجل خطة حماية النسخ (مفتاح الحماية dongle جهاز صلب صغير يستخدم كجزء من خطة حماية النسخ). يمكن للتطبيق أن يحصل على المعلومات دون مفتاح الحماية لكنه لا يقوم بتحليلها.

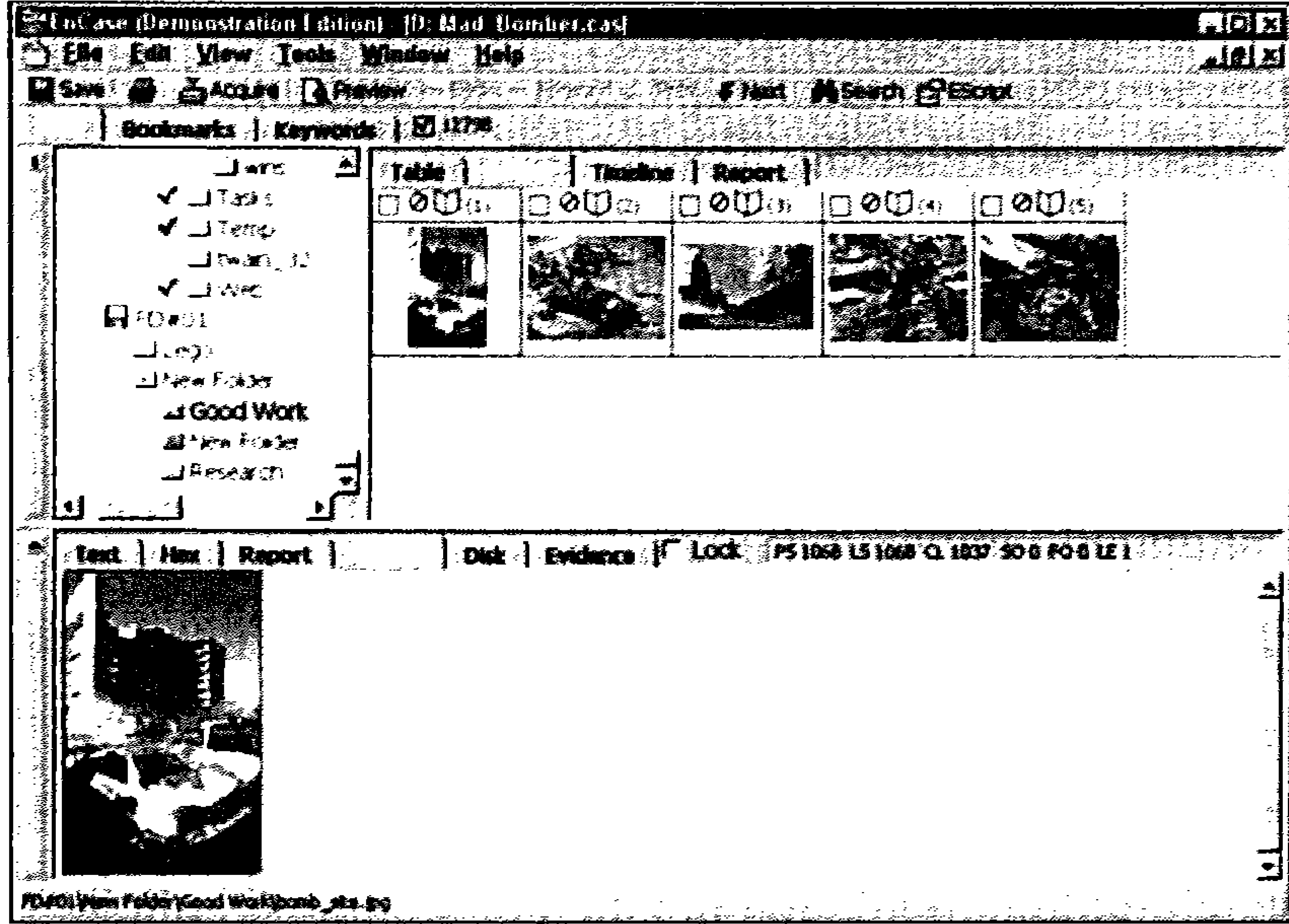
ينشئ البرنامج قرص إقلاع DOS، يستخدم على الحاسب الذي سيتم فحصه، ويصل المنفذ التفرعي، كبل مودم لا غ، أو كبل شبكة متصالب بين حاسب المشتبه به والحاسب الذي يعمل عليه برنامج EnCase. يستطيع الفاحص، بعد إقلاع حاسب المشتبه به باستخدام قرص الإقلاع وتشغيل برنامج EnCase على الحاسب الآخر، استخدام ميزة الاستعراض وذلك لرؤية محتويات حاسب المشتبه به دون أي تعديل في الدليل. تستخدم ميزة الاستعراض لتأسيس سبب محتمل أو لمجرد إجراء فحص سطحي للنظام.

كما يملك برنامج EnCase ميزة تسمى ميزة الاكتساب من أجل حفظ الدليل. فعوضاً عن القيام بمضاعفة شرعية لوسائط التخزين على الحاسب الهدف، ينشئ برنامج EnCase ملفاً يسمى ملف الدليل وهو ملف للقراءة فقط ويتضمن تمثيلاً دقيقاً للبيانات الموجودة على وسائط التخزين (تعترف المحاكم بهذه الملفات وتعتبرها دليلاً). يتم الحصول على ملفات الدليل بوصل حاسب المشتبه به مباشرة بحاسب آخر، وذلك بإزالة القرص الصلب فيزيائياً وتقييده بالقرص الصلب الخاص بمحطة عمل للاختبارات الشرعية، أو نقل البيانات عبر شبكة.

لبرنامج EnCase عدداً من الميزات لتحليل الدليل، تتضمن عمليات البحث المتقدمة للسلاسل الحرفية، بحث وعرض ملفات الرسوميات (كما هو موضح في الشكل 3-5)، فحص الملفات وذلك لتحديد فيما إذا تم تغيير لواحق الملفات بهدف إخفاء الدليل، عرض الملفات المحذوفة، وإظهار الخطوط الزمنية باستخدام معلومات الملف الخاصة بالتحكم بالوصول إلى الوسائط. يستطيع الفاحص تدوين الملاحظات حول الأدلة التي يكتشفها، لأنه يقوم بفحص الملفات والمساحة المهملة وغير المخصصة (تم شرح هذين المفهومين سابقاً في هذا الفصل). كما توجد ميزة للبرنامج وهي إنشاء تقارير مبنية على الدليل الذي تم اكتشافه.

برنامج EnCase ليس زهيد الثمن، تبلغ كلفته 2495 دولار أمريكي (1995 دولار أمريكي للوكالات الحكومية)، ولكن إذا كنت تقوم بكثير من التحقيقات، يتم تعويض الكلفة بسهولة

بالنسبة للوقت الكلي الذي توفره، ولمزيد من المعلومات عن البرنامج، تفضل بزيارة الموقع www.encase.com.



الشكل (3-5) واجهة استخدام البرنامج EnCase، تعرض ملفات الرسوميات المخزنة على القرص الصلب الهدف.

مجموعة الأدوات الخاصة بالاختبارات الشرعية FORENSIC TOOLKIT: من أحد أشهر أدوات استرداد كلمات المرور هي الأداة AccessData، والتي دخلت مؤخراً إلى سوق تحليل الأدلة بمجموعة الأدوات الخاصة بها Forensic Tollkit (FTK). تقوم مجموعة الأدوات هذه FTK بعمليات بحث متقدمة، عرض أكثر من 270 نوع ملفات، التراجع عن حذف الملفات والأقسام، وتحليل الملفات المضغوطة وملفات البريد الإلكتروني. يبلغ سعر مجموعة الأدوات الخاصة بالاختبارات الشرعية Forensic Tollkit 595 دولار أمريكي، وتتوفر نسخة تجريبية يمكنك تحميلها من الموقع www.accessdata.com.

أداة ILOOK: قد تهتم بالأداة ILook إذا كنت شرطي حاسب ذو ميزانية محدودة. تم تطوير هذه الأداة من قبل Elliot Spencer لقسم التحقيقات الجنائية التابع لدائرة ضريبة الدخل، ووزارة المالية الأمريكية، الأداة ILook مجانية "لقوى القانون فقط" وتضم عدداً من ميزات البحث والتحليل المتوفرة في المنتجات التجارية. لمزيد من المعلومات، اتبع الرابط www.ilook-forensics.org.

أساليب: خمس قواعد للدليل الناجح

توجد خمس مواصفات يجب أن يتمتع بها أي دليل إلكتروني وهي:

1. **مقبول:** يجب أن يكون الدليل قابلاً للاستخدام في المحكمة، تستطيع المحكمة أو طبيعة القضية نفسها استثناء أنواعاً محددة من الدليل وعدم عرضها في المحكمة.
2. **حقيقي:** يجب أن يظهر الدليل ارتباطه بالجريمة بشكل مباشر.
3. **كامل:** يجب أن يظهر الدليل الذي قمت بجمعه كلا جانبي الجريمة (يجب أن يثبت الدليل أن المتهم قد ارتكب الجرم، كما يعرض الوقائع التي قد تظهر براءته، وتقوم بالإشارة بحذر عن سبب اعتقادك برجحان الذنب). يعرف هذا بدليل التبرئة بين المحامين.
4. **موثوق:** يجب أن لا يكون هناك أدنى شك حول وثوقية جمعك وتحليلك للدليل.
5. **مصداقي:** كيفية تقديمك للدليل يجب أن يكون مفهوماً ومصداقياً.

إذا لم يتبع الدليل القواعد الخمسة السابقة، سيعارض القاضي أو المحامي ويختلقان نقاط ضعف في القضية. يجب تطبيق هذه القواعد على أي نوع من الأدلة، وضمن أي نوع من القضايا بما فيها القضايا المدنية والجنائية.

أدوات الفحص

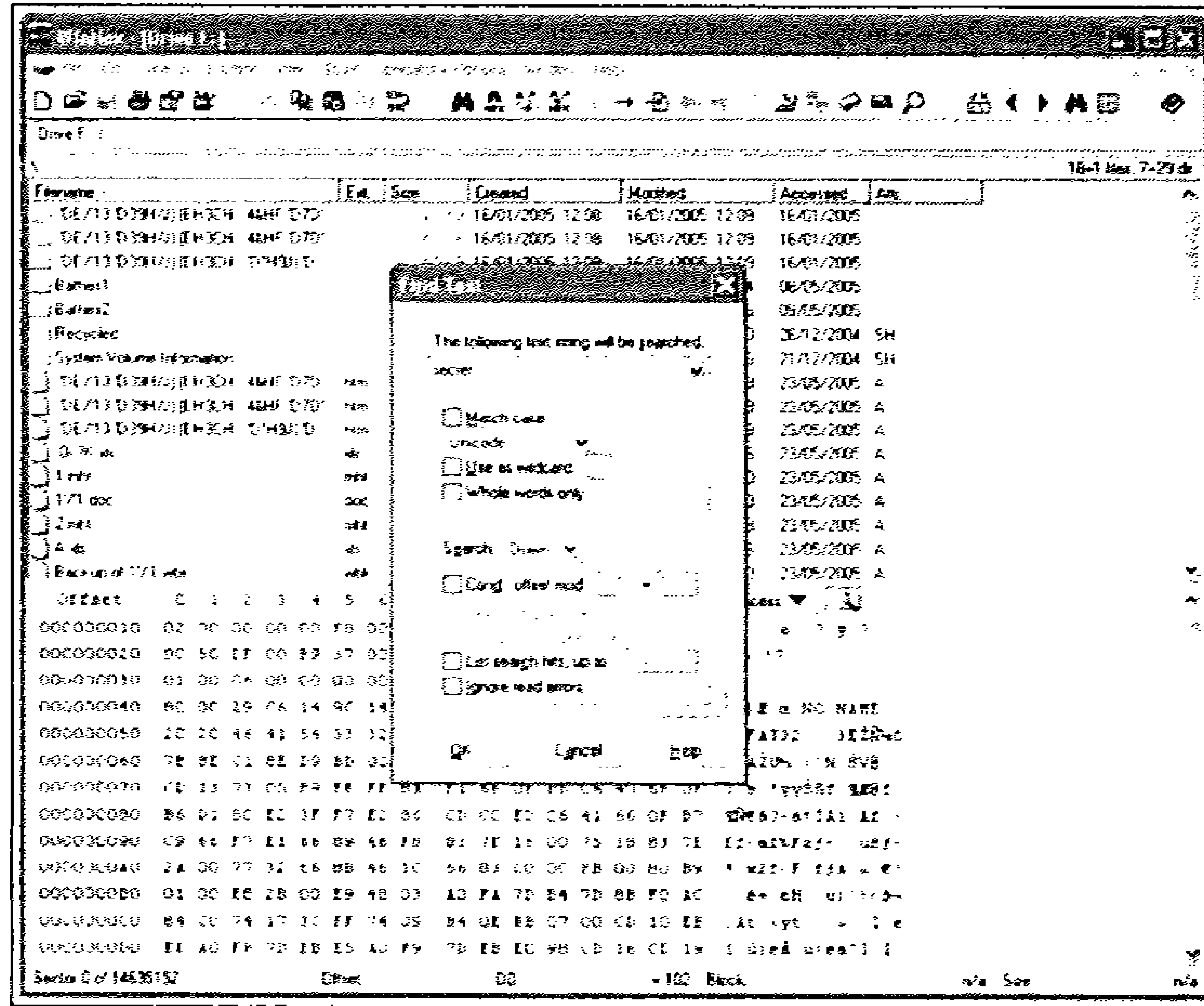
من الهام جداً أن تملك عدة أدوات عامة للمساعدة في إجراء التحقيقات، إلى جانب برمجيات جمع الأدلة المؤتمتة. يوجد نوعان هامان لأدوات الفحص التي يجب أن تستخدمها وهما:

- **محرر الأقراص Disk Editor**: كما يسمى أيضاً بالمحرر الست عشري (Hex Editor)، تتيح لك هذه الأداة إجراء عمليات البحث عن النصوص في الأقراص الصلبة ووسائط التخزين الأخرى، بالإضافة إلى فتح واستعراض الملفات بتنسيق ست عشري والتنسيق ASCII.
- **مستعرض الملفات File Viewer**: تتيح لك هذه الأداة استعراض أنواع مختلفة من الملفات دون الحاجة لاستخدام التطبيق الذي أنشأ الملف.

وفيما يلي الإصداران الشائعان لهاتين الأداتين بين رجال شرطة الحواسب والفاحصين الشرعيين:

WINHEX: بدأ برنامج WinHex كمحرر للأقراص، لكنه اكتسب عدداً من الميزات القوية على مر السنين. يمكنك باستخدام هذا البرنامج استعراض وقراءة الذاكرة، استرداد الملفات المحذوفة، النسخ المطابق للأقراص، تجميع المساحة المهملة وغير المستخدمة، إجراء عمليات البحث عن النصوص (كما هو موضح في الشكل 4-5). هذا البرنامج صغير جداً بحيث يمكن أن يتسع على

قرص مرن وحيد. يتوفر الإصدار المتخصص للبرنامج والذي يضم الميزات الإضافية للاختبارات الشرعية بسعر 100 دولار أمريكي، ويمكنك تحميل نسخة تجريبية من الموقع www.winhex.com.



الشكل (4-5) محرر الأقراص WinHex يقوم بعملية بحث عن سلسلة محرفية في القرص الصلب. تظهر النافذة الخلفية التمثيلات الست عشرية وتمثيلات ASCII للبيانات على قطاع القرص الصلب.

QUICK VIEW PLUS: أداة اختبار شائعة تقوم باستعراض وطباعة أكثر من 200 تنسيقاً مختلفاً للملفات (الرسوميات، مستندات معالجة النصوص، أوراق العمل، قواعد بيانات، عروض تقديمية، والملفات المضغوطة) بسرعة. تبلغ كلفة البرنامج 35 دولار أمريكي، كما يمكنك تحميل إصدار تجريبي من الموقع، www.jasc.com.

أدوات الاسترداد

يوجد في الأسواق عدد من أدوات الاسترداد تقوم باسترجاع الملفات المحذوفة، إصلاح المشاكل المتعلقة بوسائط التخزين التي لا يمكن الوصول إليها، واستخلاص البيانات من الوسائط التالفة. يجب أن يملك كل محقق برنامج استرداد أو أكثر في صندوق الأدوات الخاص به. من التطبيقات الشائعة:

برامج NORTON الخدمية: لقد انتشرت برامج Norton الخدمية من شركة Symantec لعدد من السنوات، ويستخدم الكثير من المحققين ورجال شرطة الحواسب هذه المجموعة، والتي تسمى "سكين الجيش السويسري"، من الأدوات المتكاملة لاسترداد الملفات والبيانات. تبلغ كلفة برامج Norton الخدمية 49.95 دولاراً أمريكياً، كما يتوفر إصدار تجريبي على موقع الشركة .www.symantec.com

الطبعة الاحترافية للبرنامج EASYRECOVERY: البرنامج الخدمي EasyRecovery Professional الخاص بشركة OnTrack هو برنامج متقدم ومكرس لاسترداد البيانات. يقوم البرنامج باسترداد البيانات من الملفات المحذوفة والمحركات التالفة، بالإضافة إلى إصلاح مستندات البرامج المكتبية Microsoft Office التالفة واسترجاع الرسائل الإلكترونية المحذوفة من برنامج Microsoft Outlook ذات اللواحق PST. و OST. (أنواع الملفات المستخدمة لتخزين بيانات البرنامج). تبلغ كلفة البرنامج EasyRecovery 499 دولار أمريكي، كما توجد نسخة تجريبية تستعرض أنواع الملفات التي يمكن استردادها (دون استرجاعها) من الرابط www.ontrack.com.

الإجراءات المضادة

لا تهدف هذه الفقرة إلى التحايل على القضاء وذلك بالتفوق على رجال شرطة الحواسب، لكن الحقيقة هي أن معظم الأشرار الأذكياء تقنياً لديهم معرفة مسبقة حول تقنيات التشفير، ماسحات الملفات، ومدمرات الدليل الأخرى. إذا كنت شرطي حواسب أو فاحص شرعي، يتوجب عليك أن تحذر من بعض هذه الإجراءات المضادة في حال صادفتها خلال عملك. في بعض الحالات التي يتم فيها استخدام الإجراءات المضادة بصورة صحيحة، قد تضطر إلى التركيز على أجزاء أخرى من التحقيق والتي لا تعتمد على الحاسب بصفته مصدراً للدليل. (الأنباء السارة هي أن معظم الإجراءات المضادة هذه تتطلب إجراءات نظامية طوال الوقت، ومعظم المجرمين كسالى في هذا الخصوص وغير أذكياء. لاحظ أعداد الجرائم التي تم حلها باستخدام بصمات الأصابع، إن ما أحاول قوله هو إذا لم يكن باستطاعة المجرم أن يتبع إجراءً بسيطاً جداً كارتداء القفازات، أعتقد أنه لن يبدأ فجأة باستخدام الإجراءات المضادة التقنية للتغلب على الشرطة).

وفي حال لم تكن شرطياً (أو مجرماً لا يرغب بأن يتم القبض عليه)، فمن الهام جداً فهم أن جاسوس ما مرتبط بالتنصت غير الشرعي سيستخدم نفس التقنيات التي يستخدمها الشرطي لمحاولة استخلاص المعلومات والدليل من حاسبك الشخصي. قد ترتبط بنشاطات شرعية وصحيحة تماماً وترغب في تطبيق البعض من هذه الإجراءات لتؤمن الحماية من التجسس غير المسموح.

التشفير Encryption

لا بد أنك قد سمعت بما يسمى بالتشفير، يمكننا ببساطة شديدة تعريف التشفير بأنه استخدام خوارزمية رياضية لتحويل المعلومات المقروءة والمفهومة إلى بيانات لا يمكن فهمها دون استخدام المفتاح الصحيح (كلمة مرور، بطاقة ذكية، أو رمز آخر). سنعرّف بعض المصطلحات، التشفير Cryptography وهو علم إنشاء الرموز السرية والشفرات. تحليل الشيفرة Cryptanalysis وهو علم اختراقها، ومصطلح Crypto باللغة العامية الأمريكية ويشير إلى أي شيء مرتبط بالمصطلحين السابقين.

لن نتعرض خلال هذه الفقرة إلى أساسيات عمل أنظمة التشفير، آثار تشفير الكم، أو أي من القضايا التقنية المرتبطة بالتشفير (والتي قد تحتل كتباً بكاملها). بدلاً من ذلك سنعرض ملخصاً سريعاً لتاريخ التشفير الحديث، بعض التوجيهات لاستخدام تطبيقات التشفير، وقائمة بمنتجات التشفير المفضلة.



لتتعلم أكثر عن التشفير، قم بزيارة المواقع التالية: موقع التشفير هذا يملك روابط عامة للمعلومات عن التشفير (http://world.std.com/~franl/crypto.html)، ويقدم هذا الموقع نشرات إخبارية شهرية ممتازة حول الأمن والتشفير (www.counterpane.com/crypto-gram.html)، ويقدم مركز الديمقراطية والتقنية مفهوم التشفير من وجهة نظر القانون (www.cdt.org/crypto/).

ملخص سريع جداً عن التاريخ الحديث للتشفير

احتكرت الحكومات التشفير حتى أوائل التسعينات، كانت تصنع الشفرات وتخترقها. استخدمت الصناعة المصرفية معيار تشفير البيانات (DES, Data Encryption Standard)، وامتلكت وكالة الأمن القومي والأعضاء الآخرون من المجتمع الاستخباراتي الأمريكي قفلاً لجميع الأمور المتعلقة بالتشفير.

خرج مارد التشفير من القمقم في منتصف التسعينات، وذلك بفضل البرنامج الخدمي الخاص بالتشفير PGP (Pretty Good Privacy)، وبفضل المشفّرين مثل Phil Zimmermann، Bruce Schneier، Whitfield Diffie، Ron Rivest، وغيرهم كثيرون، وفجأة استطاع العامة الوصول إلى التشفير على المستوى العسكري والذي لم تستطع حتى الحكومة اختراقه. في الحقيقة، تم تصنيف تقنية التشفير في فئة القذائف والأسلحة الأخرى، وكانت تخضع لقيود صارمة فيما يتعلق بالتصدير إلى الخارج.

لكن في الواقع، يستطيع الأشخاص الاتصال مع بعضهم إلكترونياً بسرية تامة مقلقين بذلك عدداً من الأشخاص العاملين لدى الحكومة، وخاصة عملاء مكتب التحقيقات الفدرالي، والذين ظلوا يحاولون تطبيق القضاء في أواخر التسعينات وهذا ما يسمى "وثيقة المفتاح". أي يجب أن تملك منتجات التشفير التجارية طريقة ملتوية لتستطيع الحكومة الوصول إلى البيانات المشفرة، أو امتلاك الحكومة أو طرف ثالث موثوق المفتاح المطلوب لفك التشفير، ويتم تقديمه لقوى القانون في حال إجراء تحقيق جنائي. لكن ضعفت وثيقة المفتاح كثيراً، تراخت قيود التصدير، وكان التشفير متوفراً بكل حرية لأي شخص يريد حماية البيانات، حتى في المحيط الحالي.

والآن بعد أن انتهينا من هذا الملخص السريع لتاريخ التشفير، سيتمكن عامة الناس من الوصول إلى منتجات التشفير، وإذا كنت شرطياً أو نوعاً آخر من الجواسيس أو تعمل لصالح وكالة حكومية، فلن تتمكن من اختراقها. هذه هي الحال حالياً، ويجب عليك أن تتمتع ببعض العبقرية عندما تحاول كشف دليل محمي بهذه الطريقة (سوف يقدم لك هذا الكتاب جميع أنواع الأفكار لتحقق المطلوب).

إرشادات عامة

بالرغم من أن التشفير يشكل أنباء سيئة للمتطفلين، لكنه من جهة أخرى خبر رائع لأي شخص يهتم بحماية سرية نشاطاته الشخصية أو المهنية. سيعترض التشفير القوي المستخدم مع إجراءات أمنية أخرى سبيل الجواسيس الذين يسعون لجمع المعلومات أو الأدلة.

إذا كنت تستخدم التشفير أو تريد استخدامه، يجب أن تتبع الإرشادات البسيطة التالية:

- عليك استخدام تطبيقات التشفير والتي تستعمل خوارزميات التشفير المنشورة والمنقحة (AES، 3DES، Blowfish، IDEA، وغيرها). لا تثق بالمنتجات ذات الخوارزميات الامتلاكية والسرية، هذه تكون غير موثوقة وعليك تجنبها.
- يفضّل أن تستخدم التطبيقات المفتوحة المصدر، حيث تسمح لك هذه التطبيقات مراجعة الشيفرة لاكتشاف الأخطاء الأمنية الضمنية وتسمح للأفراد المهتمين بالبرامج ذات الطرق الملتوية والتي تزود وصولاً سرياً، بفرصة لفحص وترجمة الشيفرة بنفسهم.
- طول المفتاح المستخدم 128 بت للتشفير المتناظر، و 1,024 بت للتشفير غير المتناظر (يسمى النوع الثاني من التشفير أيضاً "التعمية باستخدام المفتاح العمومي") وهما يصلحان حالياً. ويمكنك استخدام مفاتيح أطول إذا كنت مهتماً بالمستقبل.
- استخدم كلمات مرور صعبة وسياسات جيدة لكلمات المرور.

- يمكنك الاحتفاظ ببرمجيات التشفير على قرص مرن أو قرص مضغوط، وذلك حسب ظرفك الخاص. إذا تم اكتشاف تطبيق التشفير على قرصك الصلب، سيؤدي هذا إلى إثارة شكوك أحدهم أو يحاول أن يكشف التطبيق.
- ليس التشفير إطلاقة فضية لجميع أمور الأمن، وهذا من أحد أقوال Bruce Schneier المشفّر والمرشد الأمني الشهير، وهو محق في هذا. يجب أن يكون التشفير جزءً من سلسلة متعددة الطبقات من الإجراءات المضادة.

يمكن أن نقسم برمجيات التشفير إلى ثلاث فئات: تطبيقات تشفير البريد الإلكتروني، تطبيقات تشفير الملفات، وتطبيقات التشفير الآنية.

برمجيات تشفير البريد الإلكتروني

مع أنه يمكن استخدام أي من تطبيقات التشفير لإرسال الرسائل بأمان بين شخصين، لكن القاعدة الذهبية هي التطبيق PGP (Pretty Good Privacy). توجد بروتوكولات أخرى للرسائل الإلكترونية الآمنة، لكن حالياً أصبح التطبيق PGP هو المعيار للاتصالات الآمنة للبريد الإلكتروني، بسبب قبوله عالمياً واستخدامه الشائع.

PGP: لقد تم تطوير هذا التطبيق من قبل Phil Zimmermann في التسعينات، لقد اكتسب التطبيق PGP سمعة سيئة واستخداماً واسعاً لأنه لم يكن من الممكن اختراقه بسهولة حتى من قبل وكالات الاستخبارات الحكومية (لمعلومات أكثر حول التطبيق PGP، قم بزيارة موقع Phil على شبكة الإنترنت، www.philzimmermann.com). مع أنه تم تطوير التطبيق PGP في الولايات المتحدة الأمريكية وفي وقت تسوده قوانين التصدير المتعلقة بالتشفير، فقد تسرب التطبيق PGP إلى خارج أمريكا وسرعان ما انتشر في جميع أنحاء العالم عبر شبكة الإنترنت.

يستخدم التطبيق PGP ما يسمى بالتعمية باستخدام المفتاح العمومي (ويعرف أيضاً بالتشفير غير المتناظر). تعتمد التعمية باستخدام المفتاح العمومي على مفتاحين: مفتاح عمومي يتم منحه لأي شخص يرغب أن يتصل بك بشكل آمن، ومفتاح خصوصي تستخدمه لفك تشفير الرسائل التي تستلمها. (لا تستطيع أن تفك تشفير رسالة باستخدام المفتاح العمومي الخاص بأحد ما). وهذا يتعارض مع التشفير المتناظر التقليدي والذي يستخدم مفتاحاً وحيداً للتشفير وفك التشفير.

تقوم بتوليد المفتاحين العمومي والخصوصي عندما تستخدم التطبيق PGP لأول مرة (من السهل توليد المفاتيح المخزنة في الملفات). مثلاً، إذا أردت الاتصال سرياً بريم، والتي تستخدم التطبيق PGP أيضاً، تقوم أولاً بتبادل المفاتيح العمومية (يجعل التطبيق PGP تبادل المفاتيح سهلاً من خلال البريد الإلكتروني). ثم ترسل رسالة إلكترونية مشفرة إلى ريم، تقوم بكتابة

الرسالة أولاً ثم تشفرها باستخدام التطبيق PGP مستعملاً مفتاحها العمومي. والآن عندما تستلم ربم الرسالة تقوم بفك تشفيرها مستخدمة مفتاحها الخصوصي وذلك بإدخال كلمة المرور المرتبطة بالمفتاح الخصوصي.

يمكن استخدام التطبيق PGP على أي نظام تشغيل وهذا سبب آخر لانتشاره. لقد اعتمد التطبيق PGP في أيامه الأولى على نظام التشغيل DOS وكان صعب الاستخدام جداً، لكن بعد ذلك تم تطوير إصدارات سهلة الاستخدام تعمل ضمن بيئة Windows، كذلك يوجد عدد من الوظائف الإضافية المتوفرة لتطبيقات البريد الإلكتروني بحيث يتمكن التطبيق من الاندماج مع برنامج البريد الإلكتروني لديك.

توفرت الإصدارات السابقة من التطبيق PGP من شركة Network Associates، لكن في عام 2002 قررت الشركة التوقف عن تقديم هذا المنتج. بعد ذلك تم تأسيس شركة مستقلة جديدة PGP Corporation والتي طالبت بحق ملكية التطبيق PGP من شركة Network Associates في شهر تموز عام 2002، كما تخطط شركة PGP بإطلاق إصدار تجاري جديد متوافق تماماً مع نظام التشغيل Windows XP في نهاية العام. لمعلومات إضافية عن شركة PGP قم بزيارة موقع الشركة www.pgp.com.

يمكنك تحميل إصدارات مجانية مفتوحة المصدر للتطبيق PGP، والتي تفتقر إلى بعض الميزات الموجودة في الإصدارات التجارية من الموقع التالي، www.pgpi.org.

GNUPG. GNU هي اختصار للعبارة "GNU's Not Unix"، بدأ مشروع GNU في عام 1984 لتزويد نظام تشغيل شبيه بالنظام Unix ومؤلف من برمجيات مجانية (اتبع الرابط www.gnu.org لمعلومات أكثر عن المشروع). نشأ GnuPG (Gnu Privacy Guard) بروح GNU والبرمجيات المجانية المفتوحة المصدر (ملتزمة بترخيص الشعب العام الخاص بمنظمة البرمجيات المجانية Free Software Foundation).

من أحد القضايا التي تخص التطبيق PGP الأصلي هي استخدام خوارزميات مرخصة من شركة RSA (شركة أمن حصلت على عدد من براءات الاختراع الخاصة بالتشفير)، ومن خوارزمية التشفير IDEA (International Data Encryption Algorithm)، الخوارزمية الدولية لتشفير البيانات) الحاصلة على براءة الاختراع. بينما كان الهدف الأساسي لتصميم GnuPG هو عدم الاعتماد على شيفرة برمجية تملك قيوداً قانونية، والتمتع بالتوافق العام مع التطبيق PGP. التطبيق GnuPG هو برنامج سطر الأوامر حالياً، مع وجود بعض الوظائف الإضافية والتي تعمل على نظام التشغيل Windows. يمكنك تحميل التطبيق والحصول على معلومات إضافية من الرابط www.gnupg.org.

برمجيات تشفير الملفات

على خلاف تشفير البريد الإلكتروني والذي يهدف إلى حماية سرية الرسائل التي يمكن اعتراضها، تقوم من خلال برمجيات تشفير الملفات بحماية البيانات المخزنة على قرصك الصلب، الأقراص المضغوطة، أو أي نوع آخر من وسائط التخزين.

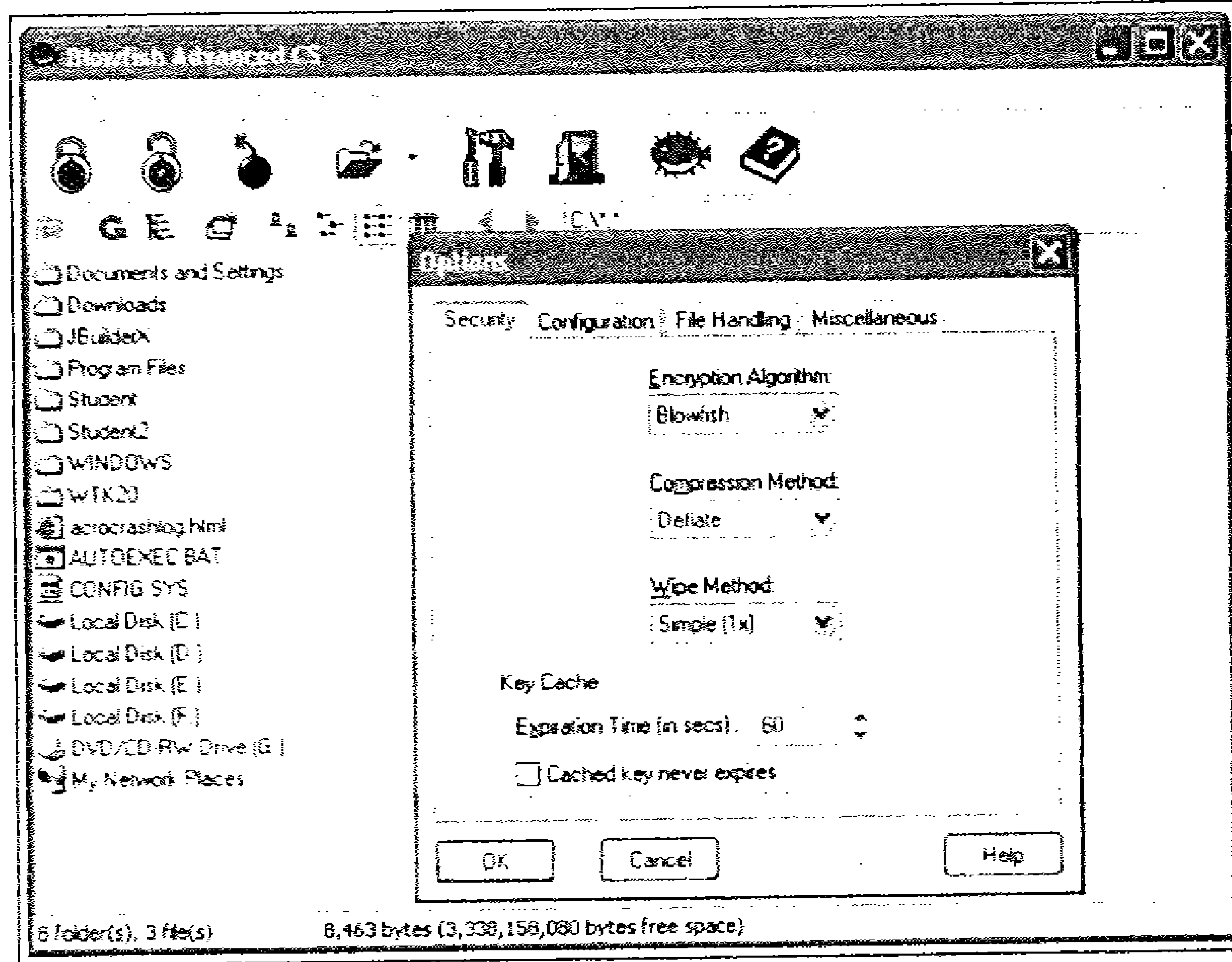
تستخدم هذه البرمجيات التشفير المتناظر التقليدي. حيث يتم استخدام مفتاح وحيد لتشفير وفك تشفير البيانات. تقوم من خلال تطبيق تشفير الملفات بتشفير الملف ومن ثم فك تشفيره مرة أخرى عندما تريد استخدامه. فعلى سبيل المثال، إذا كان لديك ملف ورقة عمل يحتوي معلومات مالية بالغة الدقة، بعد انتهائك من العمل على هذا الملف قمت بحفظه وتشفيره، وعندما تعود لتعمل على الملف مرة أخرى تقوم بفك تشفيره ليتمكن برنامج أوراق العمل من فتحه ثانية. والآن إذا تسلل أحد ما إلى قرصك الصلب، فلن يتمكن من فتح الملف واستعراض معلوماتك المالية ما لم يملك كلمة المرور.

يقدم التطبيق PGP أيضاً خدمة التشفير المتناظر للملفات، لكنه يفتقر إلى عدد من الميزات المتقدمة والتي تسهّل عملية التشفير وفك التشفير. يوجد بديلان آخران سنقوم بتقديم شرح عنهما في الفقرات التالية.

BLOWFISH ADVANCED CS: وهو برنامج خدمي، مجاني، ومفتوح المصدر طوّره Markus Hahn. يقوم البرنامج بتشفير الملفات والمجلدات باستخدام إحدى عشرة خوارزمية تشفير حديثة (بالتأكيد من بينها خوارزمية Blowfish)، كما هو موضح في الشكل 5-5. كما يتضمن التطبيق ميزة مسح الملفات وعدد من الميزات الأخرى لمعالجة الملفات. هذا البرنامج صغير الحجم بحيث يمكن تخزينه مع الملفات المطلوبة على قرص مرن وحيد مما يجعله سهل التنقل. يمكنك تحميل البرنامج الخدمي Blowfish Advanced CS من الموقع:

http://members.tripod.com/markus_hahn/software.html.

ABI-CODER: وهو تطبيق تشفير ملفات معروف ويستخدم الخوارزميات Blowfish، 3DES، وAES. يقوم البرنامج بتشفير عدة ملفات ومجلدات ويملك ميزة إنشاء ملفات آمنة، يتم فك تشفيرها تلقائياً. يمكنك تحميل الإصدار الكامل للبرنامج من www.abisoft.net/bd.html. إذا أردت الحصول على ترخيص البرنامج، يطلب المبرمج كلفة 12.99 دولار أمريكي كرسم للترخيص.



الشكل (5-5) يعرض التطبيق Blowfish Advanced CS خوارزميات التشفير التي يمكن أن يختارها المستخدم.



للحصول على تطبيقات أمن وتشفير مجانية أخرى، تحقق من فقرات الأمن Security والسرية Privacy من خلال الرابط www.webattack.com.

برمجيات التشفير الآنية OTF (on-the-fly Encryption Software)

المشكلة الأساسية لتطبيقات تشفير الملفات هي عملية الاختيار اليدوي للملفات أو المجلدات المرغوب تشفيرها، ثم عليك تشفيرها، ومن ثم عليك فك تشفيرها عندما تريد استخدامها مرة أخرى.

يحل التشفير الآني OTF هذه المشكلة وذلك عن طريق إنشاء قرص آمن ومشفر على قرصك الصلب أو أية وسائط تخزين أخرى. يمكنك باستخدام هذه البرمجيات إنشاء قرص ذو حجم ثابت، والذي يتم تشفيره بعدئذ، ويمكن إدخال القرص فقط عند تشغيل التطبيق الآني وإدخال كلمة المرور الصحيحة. والآن بعد الانتهاء بنجاح من عملية إدخال القرص، يمكن نقل الملفات الموجودة إلى القرص أو حفظ ملفات جديدة عليه، مع تنفيذ جميع عمليات التشفير وفك التشفير بشكل غير ملحوظ. تتمتع معظم البرمجيات الآنية OTF بميزات لتفريغ القرص آلياً وذلك بالضغط على تركيب مفتاحي معين أو بعد مرور فترة زمنية محددة.

توّفر حزم التشفير الآني الكثير من الوقت والجهد، لأنك لا تقوم بتشفير وفك تشفير الملفات والمجلدات يدوياً طوال الوقت، كما تسعى البرمجيات لتكون سهلة الاستخدام: حيث يظهر لديك بعد تثبيت البرنامج قرص صلب جديد أو محرك أقراص مرن آخر مُدخَل للنظام فيما يتعلق بإدارة الملفات.

مجموعة البرامج الأمنية STEGANOS: وهو تطبيق أوروبي شائع يتضمن برنامجاً خدمياً للتشفير الآني، ماسح الملفات، مزيل الأدلة، وعدد من الأدوات الأمنية الأخرى. يستخدم هذا التطبيق خوارزميات التشفير القوية مثل AES، وBlowfish وهو سهل الاستخدام جداً. تبلغ كلفة مجموعة البرامج الأمنية Steganos 29.95 دولار أمريكي، مع توفر إصدار تجريبي على الرابط www.steganos.com.

BESTCRYPT: من أقدم برامج التشفير الآنية الخدمية التجارية، ويزود تشفيراً سلساً باستخدام الخوارزميات AES، GOST (معيار التشفير الروسي)، Blowfish، و Twofish. تسوّق الشركة المصنّعة Jetico إصدارين للبرنامج BestCrypt إصدار خاص بنظام التشغيل Windows وآخر خاص بنظام التشغيل Linux، وبالتالي حاويات الملفات المشفرة تكون متوافقة بين أنظمة التشغيل المختلفة. تبلغ كلفة البرنامج 89.95 دولار أمريكي، مع توفر إصدار تجريبي على الرابط www.jetico.com.

DRIVECRYPT. برنامج خدمي تجاري لتشفير الأقراص، وهو مطوّر من التطبيقات المفتوحة المصدر والمجانية وهي Scramdisk، و E4M. يمكنك تحميل التطبيق Scramdisk (يعمل ضمن بيئة Windows 9x/ME) والتطبيق E4M (وهو اختصار للعبارة Encryption for the Masses أي التشفير للجمهور، ويعمل ضمن بيئة Windows NT/2000/XP) من الرابط www.samsimpson.com/scramdisk.php. هناك إصدار آخر بالإضافة إلى المنتج الأساسي يستخدم رمز منفذ USB (الممر التسلسلي العالمي Universal Serial Bus) كمفتاح، وإصدار آخر يقوم بتشفير كامل القرص الصلب. تبدأ كلفة المنتج من القيمة 49.95 دولار أمريكي، ويمكنك الحصول على مزيد من المعلومات وتحميل إصدار تجريبي من الرابط www.drivecrypt.com.

الإجراءات المضادة: نظام الملفات المشفر EFS

يملك نظام التشغيل Windows 2000/XP Professional ميزة تسمى نظام الملفات المشفر EFS (Encrypted File System)، وهو إصدار شركة Microsoft للتشفير الآني OTF ويسمح

للمستخدم بتشفير الملفات والمجلدات بشكل سلس، مع توفر المستندات للشخص الذي يسجل الدخول بنجاح تحت اسم حسابك. هناك نقطتي ضعف أساسيتين لنظام الملفات المشفر EFS تحت بيئة Windows 2000:

- تم إصدار النسخة الأصلية لنظام التشغيل Windows 2000 مع تشفير يبلغ طوله 56 بت وذلك لتحقيق متطلبات التصدير، وهو تشفير ضعيف جداً من وجهة نظر الأمن. فإذا كان لديك إصدار قديم من نظام التشغيل Windows 2000، يجب أن تحدثّه على الأقل إلى الإصدار Service Pack 2 وتثبيت حزمة التشفير المتقدمة ذات مفتاح يبلغ طوله 128 بت، والتي يمكن تحميلها من الرابط:
www.microsoft.com/windows2000/downloads/recommended/encryption/.
- يمكن لأي مستخدم يتمتع بامتيازات مدير النظام، في جميع إصدارات النظام Windows 2000، أن يتمكن من الوصول إلى الملفات والمجلدات المحمية دون كلمة مرور. تم تغيير هذا الأمر في النظام Windows XP Professional، والمستخدم الذي يقوم بإدخال كلمة المرور الصحيحة يستطيع الوصول إلى البيانات المحمية.

مع أن نظام الملفات المشفر EFS يبدو جيداً على الورق ولم يتم اكتشاف أي ثغرات أمنية هامة، ربما تفضّل استخدام تطبيق مستقل من طرف ثالث لحماية ملفاتك، وذلك بسبب سمعة شركة Microsoft الأقل من ممتازة فيما يتعلق بالأمن والحقيقة هي أن نظام التشفير مندمج بإحكام بنظام التشغيل (حيث يمكن أن تستدعي الأخطاء المعروفة وغير المعروفة التكاملية).



ألّفت Sarah Dean قائمة شاملة (لكنها قديمة قليلاً) لبرمجيات التشفير الآنية OTF Encryption Software، تتوفر على الرابط:
www.fortunecity.com/skyscraper/true/882/Comparison_OTFCrypto.htm.

Steganography

Steganography هو علم وفن إخفاء الرسائل السرية عن طريق تحويلها إلى شكل آخر يكون عادة ظاهراً بحيث يراه الجميع. لا يعتبر مفهوم Steganography ، باختصار "Stego"، جديداً.

- كان اليونان القدماء، منذ حوالي خمسة وعشرين ألف عام، يزيلون الشمع من ألواح الكتابة ويحفرون الرسائل ضمن الخشب الواقع في الطبقة الدنيا، ومن ثم كانوا يضعون طبقة جديدة من الشمع على الخشب وذلك لإخفاء الرسالة. وكانوا أيضاً يضعون رسائل على شكل وشم على رأس العبد الأصلع ومن ثم يدعون شعره ينمو قبل إرساله لتسليم الرسالة السرية.

- استخدم كلا الطرفين، خلال الحرب العالمية الأولى، ستيجو لتبادل رسائل الجواسيس. فعلى سبيل المثال، أرسل عميل ألماني الرسالة التالية، " Apparently neutral's protest thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts ejecting suets and vegetable oils." ربما تجد هذا غامضاً قليلاً لكن إذا أخذت الحرف الثاني من كل كلمة، ستنتج الرسالة التالية ".Pershing sails from NY June 1"
- طور الألمان، خلال الحرب العالمية الثانية، النقطة الصغرية microdot وهي تقنية تقوم بتقليص الرسالة إلى حجم النقطة في الآلة الكاتبة، ويتم إضافة النقطة الصغرية إلى نقطة في نهاية الجملة، والشخص الذي يستلم الرسالة هو الوحيد الذي يعرف بوجودها.

تعتمد الأدوات الحديثة لعلم Steganography على الوسائط الرقمية لإخفاء المعلومات. مثلا، يمكنك التقاط صورة رقمية وتخزينها كملف لاحقته JPG. وتقوم بتضمين رسالة نصية سرية في الصورة باستخدام برنامج خاص. تظهر الصورة عادية عندما يتم فتحها باستخدام تطبيق للصور. يتم اكتشاف الرسالة من قبل شخص يعلم بوجودها فقط مستخدماً برنامجاً خاصاً لاستخلاصها. تخدم ملفات الصوت والصورة بشكل جيد لتطبيق Steganography، حيث تدعم تنسيقات الملفات لديها البتات ذات الترتيب المنخفض والتي يمكن استخدامها لإخفاء محتويات الرسالة مع تشويه ضئيل جداً (غير ملاحظ) للملف الأصلي. وفيما يلي بعض أنواع الملفات والتي تستخدمها تطبيقات Steganography:

- .AU
- .BMP
- .GIF
- .HTML
- .JPG
- .MP3
- .PCX
- .PDF
- .PNG
- .WAV

يمكن إخفاء المعلومات أيضاً ضمن ملفات نصية، مثل رسالة الجاسوس الألماني في الحرب العالمية الأولى. ومثال على هذا هو الموقع SpamMimic، حيث تقوم بإدخال رسالة قصيرة ويقوم الموقع

بإخفاء المعلومات وتظهر بصورة رسالة إلكترونية لا طائل منها. ومن ثم تقوم ببساطة بنسخ الرسالة إلى تطبيق البريد الإلكتروني لديك (أو يفضل استخدام حساب ويب صعب التعقب للبريد الإلكتروني) وأرسل الرسالة للشخص المطلوب. عندما يستلم الطرف الآخر رسالتك يقوم بزيارة الموقع SpamMimic من أجل فك تشفير الرسالة. بإمكانك زيارة الموقع www.spammimic.com.

يمكن استخدام Steganography كإجراء مضاد لجمع الأدلة وذلك عن طريق إخفاء أجزاء من المعلومات ضمن مستندات أخرى. قد يكون هذا الأمر حرجاً في البلاد التي تملك برمجيات تشفير غير مرخصة أو في مواقف حيث يكون استخدام برامج التشفير مثيراً للشكوك ويتبعه تدقيق لاحق.

أساليب: آمال زائفة

انبثق علم Steganography من عالم الجواسيس المبهم، في شهر شباط (فبراير) عام 2001، واحتل الصفحات الأولى في الجرائد. أعلنت صحيفة USA Today أن أسامة بن لادن كان يستخدم Steganography للاتصال بعملائه عبر شبكة الإنترنت، كما استخدم تنظيم القاعدة ملفات الصور لإخفاء المعلومات بكل وضوح عن طريق أكثر من ملياري موقع ويب وحوالي 28 مليار صورة منتشرة عبر شبكة الإنترنت.

وبعد أحداث الحادي عشر من أيلول (سبتمبر) المثيرة للجدل، أثيرت الشائعات ثانية، حيث وردت تقارير تقول بأن أتباع أسامة بن لادن كانوا يتبادلون مئات الرسائل الإلكترونية المخفية ضمن صور رقمية عبر خدمة المزايدة الإلكترونية eBay، كما تضمن الموقع الديني Azzam.com صوراً تتضمن نصاً مخفياً، كان يوجد رابط بين الصور المشبوهة وحركة الإنترنت من مقاهي الإنترنت في باكستان والمكتبات العمومية عبر العالم.

لكن من جهة أخرى، لم يصرّح أحد من الضباط الحكوميين بصورة رسمية أن تنظيم القاعدة أو أية مجموعات أخرى كانوا يستخدمون Steganography. (ربما كان هذا صحيحاً إلى حد ما، لكن وسائط الإعلام تلعب دورها في تضخيم الأمور).

ترأس Niels Provos، مطوّر حواسب في جامعة Michigan، دراسة لإيجاد ملفات صور تتضمن معلومات مخفية ضمن المجموعات الإخبارية USENET في شهر تشرين الثاني (نوفمبر) عام 2001، حيث أن نشر رسائل مخفية عبر المجموعات الإخبارية USENET هو طريقة اتصالات أكثر أماناً، بسبب صعوبة تحديد وكشف الشخص الذي أرسل الرسالة والشخص الذي قام باستلامها. فحص فريق Provos أكثر من مليوني صورة ولم يجدوا أي دليل لرسائل مخفية في أي من الملفات.

يمكنك قراءة تقرير البحث الخاص بالدراسة السابقة من الرابط:
www.citi.umich.edu/u/provos/stego/usenet.php.

إذا كنت من مستخدمي Steganography، عليك معرفة بعض الأمور:

- لا تترك أي دليل يشير أنك كنت تستخدم برنامج Steganography. إذا وجد محقق ما نسخة من الأدوات S (برنامج مشروح في الفقرة التالية) على قرصك الصلب، فسيشك بالتأكيد بوجود ملفات تتضمن معلومات مخفية.
- عليك تشفير جميع الرسائل أو المعلومات التي تقوم بإخفائها.
- عليك اختيار الملف الحامل للمعلومات بحيث لا يثير الشكوك، مثلاً استخدام رسالة مخفية ضمن ملف صوتي ذو الامتداد MP3 ونشره عبر شبكة الند للند لمشاركة الملفات، هي طريقة أفضل من تبادل رسالة إلكترونية مخفية ضمن صورة لكوكب المشتري مثلاً.
- لا تستخدم ملفات شائعة ومنتشرة في كل مكان، لكي لا يتمكن خصمك من مقارنة الفروق بين ملفك والملف الأصلي. مثلاً، يجب عدم استخدام صورة منتشرة عبر الإنترنت كملف حامل للمعلومات السرية.
- لا تضع كل البيض في سلة واحدة، إذا كنت تواجه وكالة استخبارات حكومية. في عام 1999، شرح كل من Andreas Westfeld وAndreas Pfitzmann (http://os.inf.tu-dresden.de/~westfeld/publikationen/ihw99.pdf) كيفية تحليل الصور بصرياً وإحصائياً وذلك للكشف عن وجود رسائل مخفية. وفي جامعة Michigan، طوّر Niels Provos برنامجاً خدمياً يسمى Stegdetect والذي يكشف وجود رسائل مخفية باستخدام عدد من أدوات Steganography المعروفة (يمكنك تحميل البرنامج من الرابط www.outguess.org). لكن لا تعتقد أن الوكالات الحكومية تملك قدرات عظيمة لكشف الأنواع المختلفة لعمليات Steganography الرقمية.

هناك عدد من أدوات Steganography، لكن يمكنك باستخدام الأداتين التاليتين أن تختبر بنفسك عملية Steganography وتفهم بشكل أفضل كيفية عملها.

الأدوات S (S-TOOLS)

برمجها Andrew Brown، وهي من أحد أول أدوات Steganography المطوّرة لنظام التشغيل Windows. وهي أداة فعالة وسهلة الاستخدام، بالرغم من أنه لم يتم تحديثها منذ عدة

سنوات. تقوم الأدوات S بإخفاء الملفات ذات اللواحق BMP، GIF.، وWAV. إما باستخدام نص صريح أو مشفر. والأمر الجيد هو أن هذه الأدوات مجانية ويمكنك تحميلها من الرابط ftp.uni-stuttgart.de/pub/rus/security/win95/s-tools4.zip.

أداة WBSTEGO

يقوم برنامج wbStego4، المطوّر من قبل Werner Bailer، بإخفاء البيانات داخل صور نقطية، ملفات نصية ذات التنسيق ASCII وANSI، ملفات ذات اللاحقة HTML.، وملفات البرنامج Adobe Acrobat ذات اللاحقة (PDF.). واجهة البرنامج سهلة الاستخدام ويدعم البرنامج التشفير. تكلفة هذه الأداة 20 دولار أمريكي ويمكنك تحميل نسخة تجريبية من الرابط http://wbstego.wbailer.com/.



يمكنك الحصول على قائمة شاملة عن برمجيات Steganography من خلال الرابط http://stegoarchive.com.

برامج مسح الملفات

من الواضح، أنك لا تستطيع الاعتماد على نظام التشغيل Windows لتزيل الملفات بحيث لا يمكن استردادها، وإذا رغبت بالتخلص من الملفات نهائياً عليك استخدام برنامجاً خاصاً لمسح الملفات. تعمل هذه التطبيقات عن طريق كتابة بيانات جديدة فوق الملفات قبل مسح الملف الأصلي، وإذا تم استرداد الملف المحذوف فلن يتضمن أياً من بياناته الأصلية لأنه استبدل ببيانات جديدة.

توجد أربع طرق عامة لإزالة الملفات نهائياً: DoD NISPOM، DoD 5200.28 STD، Gutmann، والكتابة الفوقية باستخدام بيانات عشوائية غير حقيقية.

- يقدم كتيب التشغيل الخاص ببرنامج الأمن الصناعي القومي لوزارة الدفاع الأمريكية، The Department of Defense (DoD) National Industrial Security Program Operating Manual (NISPOM)، إرشادات عامة حول كيفية تنظيف مختلف وسائط التخزين (يتوفر إصدار من هذا الكتيب على شبكة الإنترنت على الرابط www.dss.mil/isec/chapter8.htm). لتنظيف الأقراص الصلبة يمكنك إزالة المغنطة باستخدام مزيل المغنطة ذو النموذج I أو النموذج II، الكتابة الفوقية للبيانات على القرص باستخدام محرف ومتممه ومن ثم محرف عشوائي وأخيراً التحقق من العملية. في حال وجود معلومات "سرية للغاية" يجب إلغاء تكامل المحرك، حرقه، سحقه، تمزيقه، أو صهره.

تستخدم معظم برامج مسح الملفات المعيار DoD لحذف البيانات نهائياً (لاحظ تصريح الحكومة بأن هذا المعيار غير كاف لمسح المعلومات "السرية للغاية").

- معيار عام 1985 لوزارة الدفاع الأمريكية DoD المعايير الموثوقة لتقدير النظام الحاسبي – 5200.28 STD، وتأتي من الكتاب البرتقالي Orange Book الخاص بسلسلة المعايير الأمنية الحاسبية "rainbow" التابعة للحكومة، وتتضمن كتابة البيانات عدة مرات فوق الملف قبل أن يتم حذفه. (من أحد الموارد الجيدة والتي تتضمن معلومات مفصلة عن تنظيف جميع أنواع وسائط التخزين، هو الدليل الخاص بأمن البحرية الأمريكية، ويتوفر على الرابط www.fas.org/irp/doddir/navy/5239_26.htm).
- أصدر Peter Gutmann، في عام 1996، مقالة تحت عنوان "الحذف الآمن للبيانات" من الذاكـــرة المغناطيسيـــة وذاكـــرة الحالـــة الصلبة[1]. (تتوفر هذه المقـــالة على الرابط www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html). افترض Gutmann أن طريقة تشفير الأقراص الصلبة يمكن أن تؤدي إلى إمكانية استرداد البيانات التي تم تطبيق عملية الكتابة الفوقية عليها سابقاً وذلك باستخدام المجهرية الإلكترونية. واقترح أن الكتابة الفوقية للبيانات ثلاثين مرة سيتغلب على هجوم خصم يستخدم مجهراً إلكترونياً، وقد تم استخدام طريقة Gutmann، بالإضافة إلى طريقة DoD، في كثير من برامج مسح الملفات.
- توجد طريقة بسيطة أخرى في برامج مسح الملفات وهي كتابة بيانات عشوائية غير حقيقية إلى وسط التخزين. تدعم معظم برامج مسح الملفات هذه الطريقة مع تحديد عدد مرات الكتابة الفوقية للبيانات.

ما هي الطريقة التي يجب أن تستخدمها لمسح الملفات؟ هذا يعتمد على أمرين، من الذي قد يكون مهتماً ببياناتك وما هي الموارد التي يملكها. يكون مسح الملفات لمرة واحدة كافياً، ما لم تخالف عملية تجسس على مستوى الحكومة. (كلما زاد عدد مرات المسح التي ينفذها البرنامج، زاد زمن تنفيذ العملية).

تشكل المجهرية الإلكترونية أحد أدوات الاسترداد التي قد يستخدمها خصم قوي وممول جيد. يشرح Gutmann في مقالته، أنه قد تبقى بعض الآثار للبيانات المغناطيسية والتي يمكن استردادها في مختبر باستخدام مجهر إلكتروني. بالرغم من أن المجهرية الإلكترونية بدون شك شكلت تهديداً عند إصدار المقالة عام 1996، إلا تشفير القرص الصلب تطور منذ ذلك الوقت، ويستخدم معظم المصنّعون حالياً تقنية قناة القراءة الموسعة Extended PRML (وهي طريقة لتشفير وفك

[1] ذاكرة الحالة الصلبة Solid-State Memory: ذاكرة الحاسب التي تخزن المعلومات في أجهزة الحالة الصلبة.

تشفير القرص الصلب) وتقنيات التصميم الحديثة. وهذا الأمر يجعل عملية استرداد البيانات أصعب بكثير من قرص صلب جديد مقابل قرص مصنّع منذ خمس سنوات.

أما بالنسبة للأقراص المرنة، فهذا أمر آخر، بسبب طريقة تشفيرها فمن الممكن استرداد البيانات الأصلية التي خضعت لعملية الكتابة الفوقية. لا تتعب نفسك وتمسح الأقراص المرنة، فقط اتبع إرشادات NISPOM وقم بتدميرها كلياً.

يوجد الكثير من برامج مسح الملفات، ومعظمها مجاني. أحد أفضل هذه البرامج هو البرنامج Eraser، برنامج مسح مجاني معروف ومفتوح المصدر، مبرمج بالأصل من قبل Sami Tolvanen. يقوم البرنامج بحذف الملفات بشكل آمن، وحذف المساحة غير المستخدمة من القرص الصلب، ويمكنك تحميل هذه الأداة من الرابط /www.heidi.ie/eraser.



للحصول على قائمة شاملة لبرامج مسح الملفات، اتبع الرابط:
www.fortunecity.com/skyscraper/true/882/Comparison_Shredders.htm.

مضبوط: Ana Belen Montes

كانت Ana Belen Montes رئيسة التحليل الاستخباراتي في وكالة الاستخبارات الدفاعية DIA (Defense Intelligence Agency) في واشنطن. بدأت Ana عملها لصالح الوكالة عام 1985، وتخصصت في عام 1992 بأمور تتعلق بكوبا. كانت تتمتع Montes بمسؤوليات مهنية تخولها الوصول إلى معلومات سرية مختلفة مما جعلها مرشحة جيدة لتكون جاسوسة لصالح خدمة الاستخبارات في كوبا CuIS (Cuban Intelligence Service).

تستخدم الاستخبارات الكوبية ما يسمى "محطات الأرقام Numbers Stations". تبث محطات الأرقام هذه سلسلة أرقام عبر ترددات الموجات القصيرة للراديو من مواقع سرية. يقرأ صوت مجهول، غالباً أنثوي، هذه الأرقام ببطء على الهواء مباشرة. تتواجد محطات الأرقام في جميع أنحاء العالم، مع قراءة الأرقام بلغات مختلفة، هذه الأرقام هي طريقة للاتصالات السرية بالجواسيس. على الرغم أن أي شخص يملك مستقبل راديو ذو الموجات القصيرة يمكنه أن يستمع، إلا أن الجاسوس فقط يستطيع فك تشفير الرسالة. (لمزيد من المعلومات حول محطات الأرقام التسجيلات الفعلية، اتبع الرابط www.spynumbers.com).

كانت Montes تتلقى تعليمات من الكوبيين عن طريق الاستماع إلى أرقام المحطة من خلال مستقبل راديو Sony ذو الموجات القصيرة، بعد الاستماع كانت تسجل الأرقام على حاسبها المحمول Toshiba ومن ثم تفك تشفير الرسائل.

شك مكتب التحقيقات الفدرالي بقيامها بالتجسس، وفي شهر أيار (مايو) عام 2001، قاموا بعملية حقيبة سوداء مرخصة من قبل المحكمة على مكان إقامتها، وتضمنت العملية إجراء مضاعفة شرعية لقرصها الصلب. قام المختصون باسترداد ملفاتها المحذوفة مما ساعد على إدانتها بتهمة التجسس، تضمن أحد الملفات النص التالي باللغة الأسبانية:

"عليك استخدام برنامج المسح وتدمير ذلك الملف وفق الخطوات التي ناقشناها خلال الاتصال. هذه خطوة أساسية عليك اتباعها كل مرة تتلقين فيها رسالة راديو أو قرص."

من الواضح أن Montes لم تتبع إجراءات عميلها المشرف، وها هي الآن تقضي مدة حكمها في السجن الفدرالي والتي تبلغ 25 عاماً.

برمجيات التخلص من الأدلة

يمكنك بالتأكيد أن تقوم بنفسك بإزالة الأدلة مثل أخطاء المستعرض الصنعية (تمت مناقشتها سابقاً في هذا الفصل)، الملفات المؤقتة، ومدخلات تسجيل النظام باستخدام ماسح ملفات، البرنامج الخدمي RegEdit، ومجموعة من الملفات الدفعية، ويوجد أيضاً عدد من البرامج الخدمية التجارية والتي تقوم تلقائياً بالتخلص من الأدلة الموجودة على قرصك الصلب. تحوي معظم هذه التطبيقات الميزات نفسها، مثل حذف أخطاء المستعرض الصنعية، حذف قوائم الملفات الأخيرة، إزالة الملفات المؤقتة، والتخلص من الأشكال الأخرى للدليل الإلكتروني. توفر هذه البرمجيات كثيراً من الوقت والجهد وخاصة عندما يتعلق الأمر بتطهير نظامك من دليل كامن.

يجب أن تتوخى الحذر من ترويج التسويق لهذه البرمجيات (أو أي برمجيات أخرى تتخلص من الدليل الإلكتروني)، حيث تزداد شعبية برمجيات التخلص من الأدلة، والبرمجيات التي تزعم أنها تحذف جميع آثارك وخاصة الإعلانات المنتشرة على مواقع الويب، ويستخدم بعضها تقنيات إعلانية مشكوك بها. عادة يكون المصنّع ذو نوايا صالحة، لكن لا يوجد أي ضمان أن أحداً لا يستطيع اكتشاف الدليل بعد أن تقوم بتشغيل البرنامج. بما أنه لا توجد أية تقارير من قبل المستهلكين لهذه الأنواع من الأدوات، فمن الأنسب أن تستخدم برنامجاً لإزالة الأدلة ومن ثم تأكد إذا كان بإمكانك استرداد أية بيانات، وخاصة إذا كان لديك معلومات هامة جداً على قرصك الصلب. نزودك خلال هذا الفصل بمعلومات وموارد وأدوات كافية، بحيث يمكنك أن تلعب دور الجاسوس وتتحقق من الإجراءات المضادة لديك. (تذكر خصم "محتمل" أو خصم "ممكن". أي لا يحتاج معظم الناس شراء مجهر إلكتروني بقيمة 50,000 دولار أمريكي ليتأكدوا فيما إذا كان بإمكانهم استرداد البيانات المحذوفة من القرص الصلب).

فيما يلي بعض تطبيقات التخلص من الأدلة المعروفة:

WINDOW WASHER

كان البرنامج الخدمي Window Washer من أوائل البرمجيات لإزالة أخطاء المستعرض الصنعية، وقد تطور حالياً ويتضمن ميزات مدمجة مثل حذف المساحة المهملة، القدرة على تنظيف ملفات ومجلدات ومفاتيح تسجيل النظام المحددة من قبل المستخدم، وموعد محدد للتنظيف الآلي من الأدلة. كما يتضمن هذا البرنامج أكثر من 150 وظيفة إضافية مجانية تعمل مع تطبيقات متنوعة لإزالة أي دليل متروك على قرصك الصلب. تكلفة هذا البرنامج 29.95 دولاراً أمريكياً ويمكنك تحميل نسخة تجريبية من الرابط www.webroot.com/washer.htm.

SURFSECRET PRIVACY PROTECTOR

يقدم هذا البرنامج ميزات متقدمة مثل التنظيف الآلي في موعد محدد، ونمط الخفية. تكلفة هذه الأداة 39.95 دولار أمريكي ويمكنك تحميل نسخة تجريبية من الرابط www.surfsecret.com.

CYBERSCRUB

تطبيق تنظيف آخر يقوم بحذف معلومات المستعرض والأدلة الإلكترونية الأخرى. تكلفة الإصدار الاحترافي للبرنامج 49.95 دولاراً أمريكياً ويمكنك تحميل نسخة تجريبية من الرابط www.cyberscrub.com.

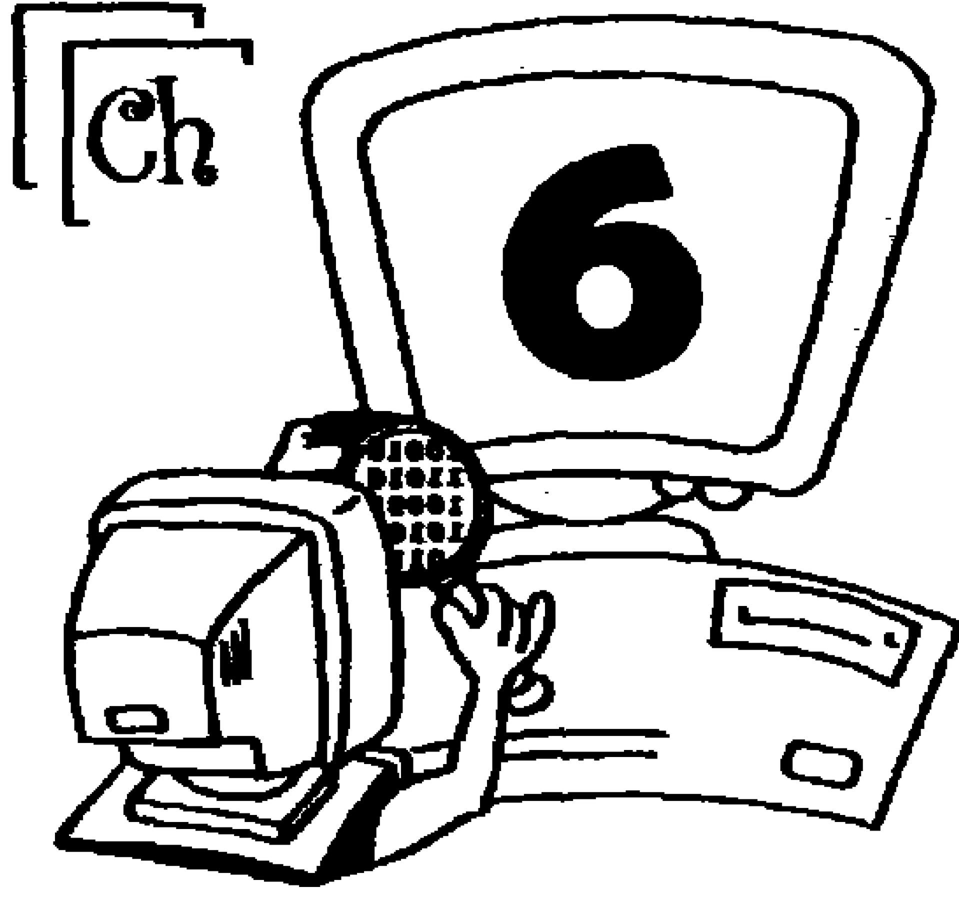
تلخيص

كما ترى هناك عدد هائل من الأدلة التي يمكن استخلاصها من جهاز الحاسب. عن طريق رجال شرطة الحواسب والفاحصون الشرعيون المحترفون عندما يتعلق الأمر بالحصول على البيانات، كما يمكن أن تُستخدم نفس الأدوات والتقنيات من قبل أي شخص مهتم في التجسس عليك.

يجب أن تتبع ثلاثة إجراءات عامة والتي سوف تحميك من الأشخاص المهتمين بجمع الأدلة من قرصك الصلب أو وسائط التخزين الأخرى لديك، وهي:

- تشفير الرسائل الإلكترونية البالغة الدقة.
- تشفير المستندات البالغة الدقة.
- التأكد من حذف أخطاء نظام التشغيل وأي تطبيق آخر.

ومن المهم أيضاً ألا تعتمد كلياً على التقنية لتصيب حاجات الأمن لديك، حيث عليك أن تضع سياسات أمنية إلى جانب الأدوات مثلاً السياسات التي تستخدم كلمات المرور، التشفير، وإزالة الأدلة. يجب تطبيق هذه السياسات والإخلاص في تنفيذها، سواء على المستوى الشخصي أو على مستوى المنظمة (السياسة هي ببساطة مجموعة من المبادئ التوجيهية، ليس من الضروري أن تكون مؤسسة ضخمة لتأتي بسياساتك الأمنية الخاصة). عليك أن تأخذ بعين الاعتبار أن معظم حالات كشف البيانات تكون نتيجة لفشل تقني مقابل فشل بشري.



إلغاء حماية البيانات

لا يعني اختراق النظام الحاسبي أنه يمكنك الوصول المباشر إلى المعلومات والأدلة المخزنة على القرص الصلب. حيث سيقوم المستخدم الذكي، الحذر، أو المرتاب والذي يهتم بسرية بياناته بتشفير البيانات، ربما باستخدام أحد الأدوات التي ناقشناها في الفصل الخامس أو على الأغلب سوف يستخدم ميزات الوقاية بكلمات المرور الموجودة في معظم الحزم البرمجية المهنية والإنتاجية.

العاملان اللذان يوقعان المستخدمين في الخطأ معظم الوقت فيما يتعلق بحماية البيانات هما التشفير الضعيف سهل الاختراق وكلمات المرور الضعيفة سهلة التوقع. يؤثر كل عامل في الآخر بشكل مباشر: حيث يبطل التشفير الضعيف كلياً كلمات المرور الصعبة، وتبرز كلمات المرور الضعيفة عدم فعالية التشفير القوي. وكل ما يحتاجه الجاسوس هو توفر أحد العاملين السابقين حتى تكون بياناتك معرضة للخطر.

سوف نناقش خلال هذا الفصل كيفية إلغاء حماية البيانات وذلك بالاستفادة من نقاط الضعف البشرية والتقنية والخطوات التي عليك إتباعها لضمان بقاء معلوماتك محمية عن الأشخاص غير المرغوب بهم.

أساليب التجسس

لا يعني تشفير الملف أنه لا يمكن كشف المعلومات داخله، حيث يعلم جاسوس الحواسب الخبير بوجود عدد من الأدوات والتقنيات للتعامل مع البيانات المحمية، لذلك سنسمح لك بالحصول على بعض من هذه الخبرة.

لننتقل الآن إلى مشهد آخر من مشاهد التشويق والإثارة، تخيل نفسك عميلاً سرياً لوكالة استخبارات ما، وقد كُلفت بمهمة التغلغل إلى داخل منظمة إجرامية دولية في بلد من بلدان العالم الثالث، وقد تعقبت أثر شخص مشتبه بتزويد الأسلحة لمنظمة ما، وبمساعدة السلطات المحلية تتمكن من الدخول إلى شقة المشتبه به لإلقاء نظرة سريعة على المكان بينما هو في الخارج لشراء بعض الأغراض. تدخل الشقة باستخدام تقنيات الحقيبة السوداء التي تعلمتها في الفصل الثالث. وتجد حاسباً محمولاً من طراز Compaq القديم قليلاً على المكتب ويعمل على نظام التشغيل Windows 95 (هذه المنظمة ليست متطورة). لقد خرج المشتبه لمدة 15 دقيقة على الأكثر، لذلك فليس لديك الوقت الكافي لتقوم بمضاعفة كامل القرص الصلب لذلك تنسخ بعض محتويات المجلدات والتي تحوي ملفات ذات أسماء مهمة على عدة أقراص مرنة. تلتقط بعض الصور الفوتوغرافية للغرفة وتخطط للعودة لاحقاً عندما يتوفر لديك مزيد من الوقت لتضاعف القرص الصلب لإجراء تحليل كامل.

تأكد من عدم ترك أي دليل يشير إلى عملية الاقتحام، واسلك طريقاً غير مباشر لتصل إلى مكان إقامتك. بعد أن تزيل قناع التنكر، تقوم بإدخال أحد الأقراص المرنة في حاسبك وتفتح أحد الملفات التي نسختها وهو ملف ورقة عمل Excel، يتم تحميل الملف لكنك تتفاجأ بصندوق حوار يطلب إدخال كلمة مرور لفتح الملف، وتتذكر بأنك لم تجد أي كلمات مرور على مكتب المشتبه به ولا تملك أي فكرة عما يمكن أن تكون كلمة المرور لذلك تضغط زر إلغاء الأمر وتغلق التطبيق. ثم تقرر فحص الملف باستخدام محرر ست عشري لمعرفة وجود بعض المعلومات التي يمكن استخدامها، لكن يتبين أن الملف مشفر بشكل ميئوس منه. كما أن جميع الملفات التي حصلت عليها مشفرة أيضاً. والأمر الأهم أن الوقت ينفذ بين يديك لأن المصادر الاستخباراتية التي تعمل لصالحها كشفت محادثات مشفرة عبر غرف الدردشة تهدد بالقيام بأعمال إجرامية قريبة، وقد تتضمن المستندات التي نسختها بعض المعلومات ذات الصلة، ولا تتوفر تجهيزات التحليل التقنية في البلد الذي تتواجد به حالياً، وتحصل تأخيرات كبيرة في إعادة الأشياء إلى الولايات المتحدة، والآن مالذي يمكنك فعله من أجل إلغاء حماية الملفات؟

استغلال نقاط الضعف

في الحقيقة يوجد لديك عدد من الخيارات لتحاول حل المشكلة التي تواجهك، حيث يمكن استغلال نقاط الضعف التقنية والبشرية لكشف المعلومات من البيانات المحمية. يجب أن تكون لديك فكرة عامة حول طريقة حماية التطبيقات للبيانات بالإضافة إلى الطريقة التي يمكن أن تقوم بها الطبيعة الإنسانية للقضاء على فعالية طريقة الحماية.

التشفير الضعيف

يتصدر التشفير الضعيف لائحة نقاط الضعف التقنية، حيث تبدو المعلومات محمية باستخدام برمجيات تشفير، لكن في الحقيقة يمكن كشف المعلومات نتيجة لعدد من العوامل:

- **خوارزميات تشفير غير آمنة.** في الحقيقة لا ينوي المبرمجون أو رؤساؤهم جعل منتجات التشفير آمنة، فإذا لم يطالب الزبائن بمستوى عالٍ من الأمن، هل يجب على الشركة أن تقلق؟ بالطبع لا. فعلى سبيل المثال، استخدمت معظم البرمجيات المهنية التي تم إنتاجها في أوائل ومنتصف التسعينات مخطط XOR بسيط (عملية حصرية أو منطقية مطبقة على النص المراد تشفيره) لحماية المستندات التي يمكن اختراقها في غضون ثوانٍ. من أقوال Eric Thompson، مؤسس برنامج AccessData ورائد في مجال عمل استرداد كلمات المرور، أنه قام بإدخال حلقات تأخير في برامجه الأولى لاختراق كلمات المرور ليعتقد الزبائن أن عملية كشف التشفير الضعيف هي عملية ليست بالسهلة وتتطلب وقتاً أكبر مما هي عليه في الحقيقة.
- **أخطاء ونقائص في خوارزمية التشفير.** وهذا أمر يختلف عن الخوارزميات غير الآمنة المذكورة أعلاه، حيث يعتقد مطورو البرمجيات بأنهم أنشئوا خوارزمية آمنة لكنهم غفلوا عن أمر ما إما دقيق أو واضح جداً. مثال على هذا، هو نظام مزج المحتوى CSS وهو اختصار للعبارة Content Scrambling System، وهو مخطط تشفير يستخدم لمزج محتوى أقراص DVD الفيديوية بحيث لا يتاح عرض هذا المحتوى إلا من خلال مشغّلات مجهزة ببرمجية فك تشفير. أتضح أن هذه الخوارزمية الامتلاكية ضعيفة جداً، عندما قام طالب نرويجي يبلغ من العمر خمسة عشر عاماً في عام 1999 بإعادة هندسة الخوارزمية وتطوير خدمة لفك التشفير تسمى DeCSS والتي اخترقت ملف DVD المشفر وحفظه بصورة غير مشفرة على القرص الصلب.
- **إصدار "الباب الخلفي" لتطبيق تشفير.** الطريقة الأخيرة لكشف البيانات المحمية هي تعديل الشيفرة المصدرية لتطبيق تشفير قوي وجعله يشفر البيانات بصورة ضعيفة (بحيث من السهل للخصم مهاجمتها) أو ربما يحفظ كلمة المرور إلى قرص. مثلاً، يمكن تعديل نسخة البرنامج PGP (Pretty Good Privacy) بحيث يستخدم أول 40 بتاً فقط من أصل مفتاح طوله 1,024 بتاً لينتج رسائل يمكن اختراقها بسهولة. ثم يقوم الجاسوس باستبدال الإصدار الأصلي لبرمجية التشفير على حاسب الهدف، بالإصدار الضعيف ويستطيع بذلك كشف أي بيانات تم تشفيرها فيما بعد.

مع الانتشار الواسع والسريع للمعلومات الجديدة عبر الإنترنت، وخاصة فيما يتعلق بالقضايا الأمنية، فمن السهل أن يبقى الجاسوس على إطلاع على الأدوات والأخطاء الجديدة لكشف

البيانات المشفرة بصورة ضعيفة. في حالة نظام مزج المحتوى CSS، حكم قاضي فدرالي في عام 2001 بمنع نشر خدمة DeCSS من قبل 2600 مجلة عبر مواقعها على شبكة الإنترنت، بالرغم من ذلك فقد انتشرت الخدمة، الشيفرة المصدرية، والتحليل المفصل للنظام CSS عبر الإنترنت، فمن المستحيل بعد ذلك إعادة المارد إلى القمقم.



يجب على كل جاسوس قراءة مقالتين غير تقنيتين حول التشفير، كتبهما Bruce Schneier، والتي تتضمن مزايا وأخطاء ومخاطر التشفير. عنوان المقالة الأولى "لماذا التشفير أصعب مما يبدو؟ Why Cryptography is harder than it looks" (www.counterpane.com/whycrypto.html) والثانية تحت عنوان "المخاطر الأمنية في التشفير Security Pitfalls in Cryptography" (www.counterpane.com/pitfalls.html).

كلمات المرور الضعيفة

من ناحية استغلال الجانب البشري يمكننا استخدام كلمات المرور، والتي تخدم كوسيلة للوثوق بالمستخدم، فإذا كنت تعرف الشخص الصحيح، يجب أن تكون الشخص الصحيح للوصول إلى البيانات. بما أن معظم التطبيقات تعتمد علي كلمات المرور لحماية المعلومات عن طريق التشفير وفك التشفير، تشكل كلمات المرور موقعاً منطقياً لهجوم الجواسيس. (نفس الأمر يُطبق عند محاولة اختراق الأمن على مستوى نظام التشغيل، كما ناقشنا في الفصل الرابع).

كلمات المرور منطقية، فهي إما صحيحة أو خاطئة. ويمكن تطبيق نفس النمطية على كونها ضعيفة أو قوية. قد تكون كلمة المرور الضعيفة هي اسم زوجتك مثلاً، أو عيد ميلاد ابنك، أي كلمة موجودة في القاموس، اسم عائلتك مع إضافة الرقم 1 إلى نهايته، أو أي تشكيل أحرف وأرقام أقل من سبعة أو ثمانية محارف. يمكن كشف كلمات المرور الضعيفة دون صعوبة بالغة، إما عن طريق توقعها أو باستخدام أداة مؤتمتة. ومن جهة أخرى لا تقع كلمات المرور القوية ضحية هذه المهاجمات.

إذا كانت كلمات المرور الضعيفة خطراً أمنياً كبيراً، لماذا يستمر الناس باستخدامها؟ للإجابة على هذا السؤال علينا أن نغوص قليلاً في أعماق النفس الإنسانية لاختيار كلمات المرور، وقد تملك القوة تأثيراً كبيراً على كلمة المرور الضعيفة.



فيما يلي بعض القراءة المفيدة للجواسيس، مع أنه قد تبدو لك المقالات قديمة جداً وتناقش كلمات المرور لتسجيل الدخول في نظام التشغيل UNIX، إلا أنها تزود أساساً لفهم عصري لمشاكل كلمات المرور. مقالة للمؤلفين Thompson، Ken، Morris، وRobert بعنوان "أمن كلمات المرور: دراسة تاريخية Password Security: A Case History" المنشورة عام 1979 (http://lambda.cs.yale.edu/cs442/doc/unix-sec.pdf)، مقالة أخرى للمؤلفين Feldmeier، David C.، Karn، Philip R. بعنوان "أمن كلمات المرور في نظام التشغيل UNIX بعد عشر سنوات UNIX Password Security Ten Years Later" المنشورة عام 1990. (http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C89/44.pdf)، ومقالة للمؤلفين Klein، Daniel V.، بعنوان "إيقاف المخرب: استقصاء حول، وتحسينات لأمن كلمات المرور .Foiling the Cracker: A Survey of and Improvements to، Password Security" المنشورة عام 1991 .(http://geodsoft.com/howto/password/klein.pdf)

كيف يختار الناس كلمات المرور: من الهام جداً فهم طريقة اختيار الناس لكلمات المرور من أجل كشف بياناتهم المحمية. مع اعتبار أن برنامج تقليدي لفحص الهجاء يمكن أن يحوي أكثر من 100,000 كلمة، ما هو دافع شخص ما أن يختار أحد هذه الكلمات أو تركيباً منها؟ لنبدأ بمجموعة من المشاهدات العامة قبل أن نتغلغل إلى نفسية المستخدم الحاسبي العادي.

- **الأمن هو عبء علينا:** يجد معظم مستخدمي الحواسب الإجراءات الأمنية مثل كلمات المرور إزعاجاً كبيراً، وسيفعلون أي شيء لتجنبها أو تقليص مقدار الوقت والجهد المطلوب للتعامل معها. ينتج عن هذا الموقف كلمات مرور قصيرة، سهلة التذكر مثل المصطلحات الشائعة أو نماذج سهلة الطباعة على لوحة المفاتيح (مثل Qwerty أو 12345).

- **ذاكرة الإنسان محدودة:** بالرغم من أن عقل الإنسان هو حاسب ضخم وقوي، إلا أنه يعاني من بعض المشاكل في قسم ذاكرة الوصول العشوائي RAM، حيث أن تذكر كلمات المرور هي من أحد المهام الصعبة علينا. وبالتالي هذا ما يجعلنا نستخدم كلمات مرور قصيرة وسهلة التذكر.

- **الحذر الأمني هو ليس من أولوياتنا:** لنواجه الأمر، إذا كنت من قراء هذا الكتاب، فإنك لست مستخدماً عادياً للحاسب، لا تملك جدار حماية على كبل المودم لديك، وتشغّل برنامج لمكافحة الفيروسات لم يتم تحديثه لمدة سنة تقريباً، ومن المحتمل أن تكون مسؤولاً عن إصابة نصف الساحل الشرقي بفيروس Klez. لا يستوعب معظم مستخدمي الحواسب

العاديين مدى تعرضهم إلى مخاطر أمنية معينة أو قد لا يهتمون بهذا الأمر بتاتاً. ثانية نعود إلى كلمات المرور الضعيفة.

منذ عدة سنوات فقط، لم تكن هناك بحوثاً كثيرة تتعلق بالنواحي النفسية لعملية انتقاء كلمة المرور. إلا أنه بدأت بعض الأعمال بالظهور في هذا المجال، وتقدم بعض الفهم العميق لجاسوس مهتم بكشف كلمة المرور لإلغاء حماية البيانات. دعونا نركز على الدراسة الأخيرة، حيث قام علماء النفس البريطانيون بتسجيل آراء أكثر من 1,200 عامل مكتب حول كلمات المرور الخاصة بهم ووجدوا بعض النتائج المشوقة.

- تم تصنيف نسبة ثلاثين بالمائة من المستخدمين تحت لقب "الهواة fans"، وغالباً يمكن التنبؤ بكلمة المرور عن طريق نمط الشخصية وبشكل أساسي على الأشياء المتوضعة على المكتب. لنفترض أنك شاهدت خلال التسلل إلى شقة المشتبه به في بداية هذا الفصل، كرة بيسبول موقّعة من قبل Seattle Mariner، إعلان لسيارة Ichiro Suzuki، ومضرب كرة موقّع من قبل Lou Pinella. واستنتج البحث البريطاني أن "الهواة" يستخدمون تشكيلة منوعة من اسم فريق رياضي أو رياضي أو شخص ترفيه حقيقي أو خيالي في كلمة المرور الخاصة بهم. مع الأخذ بعين الاعتبار هذه المعلومات والتذكارات المتعلقة بلعبة البيسبول التي رأيتها مبعثرة في أرجاء الشقة، فمن الممكن أن تبدأ بتوقّع كلمات مرور مرتبطة بلعبة البيسبول.
- كانت نسبة خمسين بالمائة من كلمات المرور مبنية على اسم أحد أفراد العائلة، الشريك، أو الحيوان الأليف. ويمكن الحصول على هذه المعلومات بسهولة كبيرة إذا عرفت كيفية عمل ذلك. تزود عمليات البحث باستخدام محرك البحث Google وشركات تسجيل الاعتماد الإلكترونية كثيراً من المعلومات عن أفراد العائلة. استنتج البحث أن هؤلاء الناس لا يتمتعون بثقافة حاسبية واسعة. يجب أن تأخذ هذا الأمر بعين الاعتبار عندما تتجسس على مستخدم خدمات شركة AOL (شركة AOL هي اختصار للعبارة America Online وهي شركة تزويد بالخدمات الشبكية على الإنترنت، وهي أحد أكبر الشركات في هذا المجال). مقابل مستخدم آخر يعمل على حاسبي Linux يتشاركان على اتصال DSL وحيد.
- تم تصنيف نسبة أحد عشر بالمائة من المستخدمين تحت اسم "المستحوذين نفسياً self-obsessed"، ويستخدمون كلمات مرور مثل "جميلة"، "قوي" يا للغرور الموجود لدى البعض، تذكر المقولة القديمة التي تقول "يذهب الكبرياء قبل السقوط"، وفي هذه الحالة تقع كلمة المرور ضمن مهاجمة القاموس لأنها شائعة جداً (مزيد من التفاصيل عن هذا في الفقرة التالية).
- تم تصنيف التسعة بالمائة من الأشخاص الباقين تحت اسم "غامضون cryptics". لم يستخدم هؤلاء المصطلحات الشائعة ككلمات مرور، بدلاً من ذلك قاموا باختيار جمل صعبة التوقع

من الأحرف والأرقام والرموز. وتملك هذه الفئة من الأشخاص خبرة واسعة في مجال الحواسب وقد تعاملوا مع إجراءات الأمن الحاسبي الأساسية. ستواجه هذا النوع من كلمات المرور عندما تتعامل مع المستخدم الذي ذكرناه أعلاه والذي ركّب شبكة Linux بمفرده.

بالطبع هناك استثناءات للمجموعات السابقة، لذلك لا تظن أن كل شخص له حساب من شركة AOL سيستخدم اسم أحد أفراد عائلته ككلمة مرور. كما ظهر موضوع مشترك نتيجة الدراسة، حتى مع تصنيفات أخرى للمستخدمين: كان تسعون بالمائة من المستجيبين للاستقصاء يملكون كلمات مرور سهلة التوقع. ذلك الرقم أكبر بكثير من الرقم الناتج عن دراسات أخرى مرتبطة بكلمات المرور الخاصة بالنظام UNIX ويمكن نسبها إلى كثافة سكانية أكبر والتي تشمل الأشخاص الماهرون تقنياً والأشخاص غير المهتمين بقضايا الأمن. هذه أنباء سيئة للمسئولين عن النظام، وأنباء جيدة للجواسيس. (لمعلومات مفصلة أكثر حول هذه الدراسة اتبع الرابط www.centralnic.com/page.php?cid=77).

كلمة المرور والبيت المبني على أوراق اللعب: لعل من بعض الأشياء التي كان يفعلها الطفل، أيام زمان، عندما كان يسأم من اللعب بالسوليتير باستخدام أوراق اللعب الحقيقية، هو بناء بيت من هذه الأوراق ويحاول جعله أكبر وأكبر، ويتطلب هذا العمل الكثير من الصبر والدقة لتتم موازنة الأوراق عند بناء الجدران والأسقف والأرضيات. وكان يجب ارتكاب خطأ وحيد صغير ويتداعى البيت الذي حرصت على بنائه للسقوط.

يطبق نفس الأمر على كلمات المرور، حيث يحث خبراء الأمن، الرؤساء في العمل، المقالات المختلفة في المجلات والكتب، المستخدمين على انتقاء كلمات مرور قوية يصعب توقعها ومقاومة لهاجمات توقع كلمات المرور اليدوية أو المؤتمتة، لكن يوجد سر صغير غالباً ما ينسون ذكره وهو: أن المستوى النهائي للأمن يعتمد على مكان استخدام كلمة المرور القوية.

لنفترض أن المتهم الذي نلاحقه يستخدم برنامج PGP لتشفير وفك تشفير بريده الإلكتروني وهو فطن بشكل كافٍ ليستخدم كلمة مرور قوية. وأنت من جهتك تريد معرفة محتوى رسالته، وقد قمت بانتزاع نسخة من مفتاحه الخاص خلال أحد أعمال الحقيبة السوداء إلى شقته، لكنك لم تستطع الحصول على كلمة المرور. لذلك بدأت بالتنصت على اتصاله بالإنترنت واكتشفت أنه استخدم كلمة المرور "D2fitHPoR>" ليسجل الدخول إلى أحد منتديات الدردشة. لقد تمت حماية مستندات Word و Excel اللذان قمت بنسخهما سابقاً باستخدام خطة تشفير خسيسة حيث يمكنك باستخدام أدوات جاهزة معرفة كلمة المرور في أقل من ثانية (وتكتشف أن كلمة المرور هي أيضاً "D2fitHPoR>"). إن كلمة المرور "D2fitHPoR>" هي كلمة صعبة التوقع، لكن ماذا لو كان المشتبه يستخدمها أيضاً مع برنامج PGP؟ صحيح! وجدتها! عندما تستخدم

كلمة المرور هذه على رسائله التي قمت باعتراضها يصبح من السهل عليك الآن فك تشفيرها. لقد نلت ميدالية تقدير لجهودك المبذولة.

إن استخدام نفس كلمة المرور في التطبيقات التي تقدم مستويات حماية قوية وضعيفة هو أمر يعرضك لخطر كبير. غالباً ما يكون استخدام نفس كلمة المرور مرات متعددة من أحد خصائص الطبيعة الإنسانية التي يمكنك استغلالها. وجدت Rachna Dhamija، الباحثة في جامعة كاليفورنيا في Berkeley، أن المستخدم العادي قد يستخدم كلمة المرور من 10 مرات إلى 100 مرة لأغراض مختلفة، لكنه قد يستخدم كلمة مرور واحدة إلى سبع كلمات مرور مرات عديدة، وعندما يتم كشف كلمة المرور سوف يقع البيت بكامله.

مضبوط: مكتب التحقيقات الفدرالي ضد المخربين من روسيا، الجزء الثاني

لقد عرضنا في الفصل الأول من الكتاب عملية احتيال قام بها مكتب التحقيقات ضد مخربين من روسيا (انظر الفقرة " مضبوط: هل هو شرطي جيد، أم سيئ؟" في الفصل الأول). لقد تم جذب الروسيين إلى أمريكا من خلال عروض العمل من شركة أمنية مزورة ومن ثم تم ضبطهما عندما قام عملاء المكتب باستخدام برنامج مسجلات مفاتيح والذي كشف أسماء الحسابات وكلمات المرور للحواسب في روسيا (ومن ثم تم الدخول إلى هذه الحواسب من قبل الاختصاصيين من أجل جمع الأدلة).

كان بحوزة أحد المشتبه بهم وهو Alexey Ivanov حاسبه المحمول من نوع Toshiba، وبعد إعلان مكتب التحقيقات عن اعتقاله، أعطى Ivanov الإذن لأحد العملاء بتفتيش حاسبه، لكن نظام الحاسب كان محمياً عن طريق كلمة مرور للنظام BIOS، طلب العميل منه كلمة المرور فقام بإعطائه لها. (قد تتفاجأ بكثرة طلب المعلومات أثناء إجراء التحقيقات).

كلمة المرور هي "FynjyKj[". وهي كلمة مرور قوية وفقاً لمعايير أي كان، لأن طولها ثمانية محارف وتضمنت تركيبة متنوعة من المحارف. كان عملاء المكتب على علم أن Alexey Ivanov له لقب "subbsta"، ولديهم عنوان أحد الحواسب البعيدة التي قام بالدخول إليها في روسيا، لكنهم لم يملكوا اسم الحساب وكلمة المرور للحاسب البعيد.

قام أحد قادة عملاء مكتب التحقيقات باستخدام خدمة Telnet (أي الوصول البعيد إلى حاسب عبر شبكة الإنترنت باستخدام بروتوكول Telnet). للاتصال بالحاسب في روسيا وأدخل اسم الحساب "subbsta" وكلمة المرور "FynjyKj["، وقد نجح ذلك وقام العميل بتسجيل الدخول إلى الحاسب الروسي. هذا مثال تقليدي لانهيار البيت المبني على أوراق اللعب المبني على معرفة كلمات مرور قوية واحدة فقط.

المهاجمات على البيانات المحمية

أسهل طريقة لمهاجمة البيانات المحمية هي إيجاد كلمة مرور تمت كتابتها على شاشة الحاسب أو مخزنة ضمن درج المكتب. انتهت اللعبة وقد أنجزت مهمتك. لكن بما أن المجرم المشتبه به لم يترك الأمور سهلة عليك وقد قام بتغيير جميع كلمات المرور وتحديث إصدار برنامج Microsoft Word، لذلك عليك الآن اكتشاف طرقاً جديدة لالتقاط كلمة المرور الجديدة. تتضمن بعض الاحتمالات ما يلي (دون ترتيب معين):

- أوامر المحكمة (على الأقل في الولايات المتحدة الأمريكية)
- الابتزاز
- الرشوة
- الجنس
- المخدرات
- المراقبة التقنية (التنصت)
- الهندسة الاجتماعية
- التعذيب (علم فك الشيفرة)

لكن بما أن هذا الكتاب يتعلق بالتجسس الحاسبي، لذلك سنتعرض لأربع طرق تقليدية لمهاجمة البيانات المحمية وهي: مهاجمات توقع كلمات المرور يدوياً، مهاجمات القاموس، مهاجمات القوة العمياء، وفك الشيفرة.

مهاجمات توقع كلمات المرور يدوياً: الطريقة الأولى التي يتوجه إليها معظم الناس عند مواجهة كلمة المرور هي ببساطة توقعها، وذلك بإجراء محاولات يدوية لكلمات مرور قد تكون صحيحة. عندما يطلب التطبيق كلمة مرور، تدخل الكلمة التي تبدو منطقية. يجب أن تعتمد مهاجمات التوقع اليدوية على أساليب سلوك المستخدم المعينة، وتتضمن ما يلي:

- **السلوك العام:** يمكن التنبؤ بسلوك معظم مستخدمي الحواسب فيما يتعلق بكلمات المرور: يستخدمون أسماء حسابهم، الكلمة "password"، لا يستخدمون كلمة مرور على الإطلاق، كلمات المرور الافتراضية، أو نفس كلمة المرور مرات عديدة. (بما أنك عميل حكومي، فسوف يكون لديك إطلاع على الميزات السلوكية لمستخدمي الحواسب الذين لا يتكلمون اللغة الانكليزية).

- **السلوك الخاص:** إذا قمت بتجميع المعلومات حول هدفك وحصلت على لمحة عن حياته، يمكنك أن تجرب كلمات مرور مثل اسم زوج أو طفل المشتبه به، رقم الضمان الاجتماعي، تواريخ الأعياد السنوية أو أعياد الميلاد، أو أي معلومات هامة أخرى قد يستخدمها الهدف وقادر أن يتذكرها. (المثال الخيالي التقليدي الذي يمكن أن نطبقه هنا هو الفلم War Games الذي انتشر في الثمانينيات، حيث يقوم Matthew Broderick باختراق حاسب NORAD مستعملاً اسم ابن العالم الميت، Joshua).

يمكن أن تكون هذه المهاجمات ناجحة بشكل غير متوقع، لكنها قد تكون بطيئة ومتعبة أيضاً لأنه عليك إدخال كل كلمة مرور متوقعة ضمن مربع حوار التطبيق، كما يوجد هناك احتمال توقف التطبيق بعد عدد محدد من المحاولات الفاشلة، فإذا لم تنجح بعد عدة محاولات أو عدة دقائق فمن المستحسن أن تستخدم مهاجمة القاموس باستخدام برمجيات متخصصة، كما هو مفصل في الفقرة القادمة. إذا جمعت معلومات مفصلة حول الهدف، فمن السهل أن تضيفه إلى لائحة من الكلمات للتوقع المؤتمت خلال تطبيق مهاجمة القاموس.



كتب Paul Bobby مقالة ممتازة حول تكوين قواميس مركزة للمساعدة في تحديد كلمة المرور الخاصة بمستخدم ما، وهذا يتضمن تجميع المعلومات عن الهدف ومن ثم خلط كلمات المرور المتوقعة اعتماداً على قواعد مختلفة. تتوفر هذه المقالة على الرابط rr.sans.org/authentic/cracking.php.

أساليب: البريد الإلكتروني الخاص بالرئيس العراقي صدام حسين!

في شهر تشرين الأول (أكتوبر) عام 2002، زار الباحث الأمني المستقل Brian McWilliams الموقع الرسمي للحكومة العراقية www.uruklink.net/iraq، وقد لاحظ أنه كان هناك رابط حيث بإمكانك إرسال رسائل إلى الرئيس العراقي صدام حسين. وحساب الإنترنت المرتبط بالرابط هو press@uruklink.net. (من غير المعروف إذا كانت الكلمة press تدل على معناها الحرفي أو هي اختصار لرئيس الجمهورية صدام President Saddam).

وقد لاحظ McWilliams وجود مستخدمين عابرين لديهم حسابات على الموقع ويمكنهم التحقق من بريدهم الإلكتروني، قام McWilliams اعتماداً على مهاجمة توقع كلمة المرور التقليدية بإدخال الكلمة "press" في حقل اسم الحساب و "press" أيضاً في حقل كلمة المرور. وبعد أن كاد يفقد الأمل تفاجأ بأن البريد الوارد لصدام قد فتح أمامه مليئاً بالرسائل.

لقد كانت الرسائل الإلكترونية منذ شهر آب عام 2002، حيث لم تفتح أية رسائل ولم ترسل ردود عليها وقد وصل البريد الوارد إلى سعته الأعظمية ولم يعد بمقدوره استقبال رسائل

جديدة. قام McWilliams بتحميل أكثر من ألف رسالة إلكترونية موجهة إلى الرئيس صدام حسين. كان هناك أنواع مختلفة من الرسائل من بينها رسائل الإزعاج، التهديد، ورسائل من المعجبين يطلبون صوراً وتواقيع. كما كان هناك رسائل من شركات أمريكية كانت قد قدمت طلباً لإجراء مفاوضات حول العمل مع الرئيس صدام حسين بهدف بيع منتجاتها أو خدماتها.

بالرغم من أن هذا الحدث قد انتشر بين وسائل الإعلام على الإنترنت، صرح McWilliams أن السلطات الحكومية لم تتصل به بشأن الرسائل التي قام بتحميلها. بملاحظة عدم اهتمام السلطات الفدرالية بالموضوع، هذا يعني أن أحد الوكالات الاستخباراتية الأمريكية كانت قد اخترقت البريد الإلكتروني للرئيس حسين وكانت تراقبه فعلياً.

غير McWilliams كلمة المرور للحساب قبل أن ينشر الخبر، ومن ثم قام شخص آخر من الموقع urulink.net بتغييرها ثانية. لم يترك انهيار نظام الحكم للرئيس صدام حسين، في شهر نيسان (أبريل) عام 2003، كثيراً من الوقت للمخربين المحليين المتطوعين اقتحام مواقع الويب العراقية الأخرى خلال الحرب. لكن تذكر أنه بالرغم من أن اقتحام الملقمات الصديقة أو المعادية قد يبدو عملاً وطنياً، لكنه لا يزال يعتبر غير شرعياً.

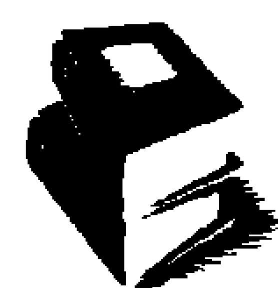
مهاجمات القاموس Dictionary Attacks: وهي طريقة أكثر فعالية من أجل كشف كلمة المرور الخاصة بأحد ما، حيث يتم من خلال هذه الطريقة التحقق من قائمة من الكلمات لمعرفة إذا كان أحدها يطابق كلمة المرور، يعتبر هذا النوع من الهجوم جيداً لكشف كلمات المرور الضعيفة المؤلفة من مصطلحات معروفة. تقدم معظم برامج كشف كلمات المرور خياراً لتحديد ملف أو أكثر من قوائم الكلمات، إما قائمة جاهزة أو قائمة تقوم بإعدادها بنفسك. يقوم البرنامج بقراءة كلمة من القائمة ومن ثم يتحقق منها في المستندات المشفرة فيما إذا كانت تطابق كلمة المرور المطلوبة لفك تشفير المستند. إذا تم إيجاد تطابق، ينتهي الهجوم ويتم عرض كلمة المرور.

هناك مئات من قوائم الكلمات المتوفرة على الإنترنت والتي تتضمن كلمات، الأسماء الشائعة، شخصيات الخيال العلمي، مصطلحات دينية، ومراجع إلى وسائل ترفيه وتسلية معروفة، الأفلام، وبرامج التلفاز. كما تتواجد أيضاً قوائم كلمات بلغات مختلفة مثل اليابانية، الروسية، الكرواتية، الفرنسية، الألمانية، وغيرها وذلك للتعامل مع أحد يستخدم لغات أخرى. إذا قمت بإجراء بحث شامل عن هدفك لا بد من أن تكون لديك فكرة جيدة عن نوع قوائم الملفات المناسبة لاستخدام مهاجمة القاموس.

تقدم الكثير من برامج التخريب ميزات متقدمة، مثل اختيار كل كلمة من القائمة المطلوبة وتكبير الحرف الأول، استبدال الحرف "o" بالصفر، أو إضافة رمز أو علامة ترقيم إلى نهاية الكلمة (جميعها وسائل شائعة قد يستخدمها شخص أكثر من عادي لجعل كلمة المرور صعبة التوقع).

تزود مهاجمات القاموس أعلى نسبة نجاح فيما يتعلق بكشف كلمات المرور —وقد أظهرت دراسات مختلفة أن نسبة تتراوح من 50% إلى 90% من مستخدمي الحواسب يعتمدون على الكلمات الشائعة لحماية بياناتهم أو لحماية الوصول إليها.

يجب أن تستخدم مهاجمة القاموس من ضمن خطواتك الأولى لإلغاء حماية البيانات، قبل أن تقوم بتشغيل الهجوم، عليك تجميع أكبر قدر ممكن من قوائم الكلمات التي تجدها وقم بنسخها إلى قرص مضغوط أو إلى القرص الصلب (هذا يجعل الهجوم أسرع بكثير نتيجة لأوقات وصول القراءة الأسرع للأقراص الصلبة).



قوائم الكلمات رخيصة ووفيرة على شبكة الإنترنت، بعض المصادر التي تقدم مجموعات مجانية قابلة للتحميل من قوائم الكلمات الإنكليزية والأجنبية والمثالية لهجوم القاموس تتضمن Access Data (www.accessdata.com/dictionaries.htm)، ElcomSoft (www.elcomsoft.com/prs.html)، وجامعة Oxford (ftp.ox.ac.uk/pub/wordlists/).

مهاجمات القوة العمياء BRUTE-FORCE ATTACKS: إذا كان هدفك ذكياً كفاية فيما يتعلق بكلمات المرور وقد فشلت محاولة مهاجمة القاموس، الطريقة التالية هي تجريب مهاجمة القوة العمياء، حيث يتم تجريب كل تركيب ممكن من الأحرف، الأرقام، علامات الترقيم، والرموز (أو مجموعة جزئية منها) في محاولة لكشف كلمة المرور. تشبه مهاجمة القوة العمياء مهاجمة القاموس ما عدا أنه يتم تجريب تركيبات مختلفة من المحارف ومقارنتها بكلمة المرور حتى يتم الحصول على تطابق بدلاً من التحقق من كلمات ضمن قائمة كلمات.

يعتمد نجاح مهاجمة القوة العمياء بشكل كامل على طول كلمة المرور، كلما كانت كلمة المرور أطول كلما قل احتمال نجاح الهجوم، في الحقيقة بعد أن تصل كلمات المرور طولاً محدداً، تمنع المتطلبات الزمنية للبحث الشامل من إمكانية نجاح الهجوم.

دعونا نقوم بحساب رياضي سريع. يوجد 95 محرف محتمل يمكن أن يشكل كلمة المرور (128 محرف ASCII ناقص 33 محرف لا يمكن طباعته، مثل محرف ASCII رقم 7 وهو محرف التحكم ctrl). كما يوجد أيضاً 128 محرف ASCII إضافي (محارف أخرى غير الأحرف النظامية،

الأرقام، والرموز، مثلاً ينتج رقم ASCII 42 الحرف Ã)، لكن معظم المستخدمين الذين يتكلمون اللغة الإنكليزية لا يفكرون أبداً باستخدام هذه المحارف في كلمات المرور الخاصة بهم (هذا يشكل بحد ذاته إجراء مضاد)، كما يمكن ألا يدعم التطبيق نفسه هذه المحارف.

لتفترض بأن المجرم الذي نلاحقه قرر أن يستخدم كلمة مرور بطول ثمانية محارف باستخدام تطبيق ذو تشفير قوي لتشفير وفك تشفير بياناته. إذا قام باختيار المحارف من محارف ASCII القابلة للطباعة، سوف يكون لدينا 6.6×10^{15} تركيباً فريداً لنختار منها، إذا قررت أن تستخدم مهاجمة القوة العمياء على كلمة المرور مفترضاً إجراء مليون توقع في الثانية، عليك الاعتماد على عدة أجيال قادمة من أقربائك لمساعدتك في هذا الهجوم: سيستغرق الأمر أكثر من 200 سنة لتجريب جميع التركيبات الممكنة. (بالطبع هذا الأمر ليس عاملاً في قانون Moore، الذي ينص على أنه يتضاعف عدد الترانزستورات في كل بوصة مربعة من الدارات المتكاملة سنوياً مما يزيد من طاقة الحاسب، أو الاختراقات الممكنة في تحليل الشيفرة).

لكن سوف نفترض حالياً أن المجرم لم يتبع الإجراءات الأمنية ويستخدم كلمة مرور بطول خمسة محارف فقط من أصل 95 محرف محتمل، هذا الأمر يقلص عدد احتمالات كلمة المرور إلى 7.7×10^{9}، وهذا سوف يستغرق أكثر بقليل من ساعتين مع تجريب مليون محاولة في الثانية، وذلك لتجريب جميع تركيبات كلمات المرور الممكنة.

يوجد، مع أية مهاجمة قوة عمياء، فكرة تتعلق بالعائدات المنخفضة المبنية على موارد الحاسب المتوفرة لديك لتنفيذ الهجوم، تطبق هذه القاعدة على الجميع بغض النظر إذا كنت تملك الوصول إلى الحاسب الفائق الخاص بوكالة الأمن القومي أو تستخدم حاسباً شخصياً عادياً، حيث عندما يبلغ طول كلمة المرور أو المفتاح حجماً محدداً سوف تكون المهاجمة غير عملية بتاتاً بسبب كمية الوقت التي سوف تستغرقها. قد لا تعرف طول كلمة المرور لكن يجب تحديد عتبة أعظمية لتقليص البحث بشكل يتعلق بمواردك الحاسبية وكمية الوقت التي ترغب بتكريسها محاولاً اكتشاف كلمة المرور.

من المهم أيضاً تحديد مدى قيمة المعلومات التي تحاول فك تشفيرها وإزالة الحماية عنها، هل هي خطيرة بما فيه الكفاية لقضاء أشهر في محاولة كشفها؟ هل سيكون لهذه المعلومات أية قيمة عندما تكشفها في النهاية؟ فعلى سبيل المثال، لنفرض أنك شرطي حواسب وقد قمت باعتراض رسالة مشفرة من أحد تجار المخدرات إلى زبونه، وقد استغرقت ستة أشهر لفك تشفير الرسالة والتي تتضمن معلومات مفصلة عن الشحن الذي حدث بعد أسبوع واحد من إرسال الرسالة. وفي النهاية هل تبرر هذه المعلومات الوقت والجهد لكشفها؟ (وسوف نفترض أيضاً أن المجرم

ذكي كفاية ليغير كلمة المرور بشكل دوري، حيث إذا تم كشف رسالة واحدة فهذا لن يؤثر على الرسائل السابقة أو القادمة).

أساليب: الأكثر أفضل

من الواضح وجود قيود تحد من تنفيذ مهاجمة القوة العمياء باستخدام حاسب وحيد. من جهة ثانية ماذا لو قمت بتجنيد حواسب إضافية خلال سعيك لكشف البيانات؟ تسمى هذه الطريقة بطريقة المهاجمة الموزعة، حيث يكون لديك الكثير من الحواسب، يعمل كل منها على أجزاء صغيرة من العدد الكلي لكلمات المرور أو المفاتيح المحتملة.

حتى أواخر التسعينات، كان معيار تشفير البيانات Data Encryption Standard (DES) هو المعيار الذهبي للتشفير، لكن بالرغم من قوة الخوارزمية تصاعدت الشكوك باطراد حول إمكانية تعرض هذه الخوارزمية إلى مهاجمة القوة العمياء، بسبب طاقة الحواسب المتزايدة. (ولقد انتشرت إشاعات منذ وقت طويل أن وكالة الأمن القومي الأمريكية تملك حواسب تستطيع اختراق خوارزمية DES).

أصدرت شركة RSA، في شهر كانون الثاني (يناير) عام 1997، سلسلة من التحديات لاختراق خوارزمية DES، مع تنوع الجوائز النقدية بحسب طول المفاتيح المستخدمة. منحت جائزة بقيمة 1,000 دولار أمريكي مقابل اختراق الإصدار الصادر من خوارزمية DES، إلى جامعة كاليفورنيا في Berkeley إلى باحث استخدم 250 محطة عمل تابعة لحرم الجامعة ليخترق المفتاح في غضون ثلاث ساعات ونصف. سوف يكون التحدي التالي أصعب بكثير، مع مفتاح بطول 56 بت، مع منح جائزة بقيمة 10,000 دولار أمريكي لأول شخص يقوم بالاختراق. (تقول قاعدة الإبهام يتضاعف عدد المفاتيح المحتملة مع كل بت إضافي).

بدأ كل من Rocke Verser، Matt Curtin، و Justin Dolske بمشروع أطلق عليه اسم DESCHALL والذي اعتمد على الحواسب المتصلة بشبكة الإنترنت للقيام بمهاجمة القوة العمياء. كان هناك أكثر من 256 مفتاح (أي أكثر من 72 مليون مليار مفتاح) والتي يجب التحقق منها. لقد تمت كتابة الشيفرة البرمجية لشتى أنواع أنظمة التشغيل ومنصات العمل والتي قد تتصل بملقم مركزي، وتحمّل قسماً من مساحة المفتاح الذي يجب البحث ضمنه، تتحقق من المفتاح، ومن ثم تعيد النتائج إلى الملقم.

بدأت مجموعات أخرى مشاريع مماثلة، لكن المشروع DESCHALL تضمن أكبر عدد من المشاركين، وخلال العملية تم تسجيل أكثر من 78,000 عنوان IP والتي ساعدت على القيام بالتحدي. في فترة 24 ساعة، كان هناك أكثر من 14,000 مضيفاً يعملون على الهجوم في نفس الوقت. أخيراً في شهر حزيران (يونيو) عام 1997، بعد التحقق من نسبة 24.6 من

مساحة المفتاح (أي 18 مليون مليار مفتاح) تم اكتشاف المفتاح في فترة 96 يوماً. (يتوفر مقال مفصل عن هذا المشروع على الرابط /www.interhack.net/pubs/des-key-crack).

بعد المشروع DESCHALL، تم إجراء مشاريع اختراق موزعة أخرى لمهاجمة مفاتيح أكبر وأكبر. لقد كان الهدف الأساسي لهذه الأحداث هو عرض نقاط القوة والضعف لخوارزميات التشفير المختلفة خلال مهاجمات القوة العمياء (يوجد أيضاً مشاريع حواسب موزعة لغير أغراض التشفير مثل المشروع SETI@home، والذي يبحث عن الحياة خارج الكرة الأرضية، والمشروع Folding@home، والذي يدرس طي البروتين وأمراض أخرى).

إذا رغبت في المشاركة بأحد هذه المشاريع، قم بزيارة الموقع Distributed.net.

تحليل الشيفرة CRYPTANALYSIS يشير هذا المصطلح إلى دراسة خوارزميات التشفير، أنظمة التشفير (أنظمة لتشفير وفك تشفير البيانات)، والنص المشفر مع هدف استرجاع النص الصريح (المعلومات غير المشفرة) من خلال المعلومات المشفرة. تحليل الشيفرة هو علم وفن معاً، حيث يقوم الأشخاص الذين يمارسون هذا العلم بمزج العلوم الرياضية، الفضول، الحدس، التصميم، والحظ لحل مشاكل التشفير.

هناك عموماً نوعان من الأشخاص الذين يخترقون الشيفرة والرموز:

- **الحكومة.** توظّف وكالة الأمن القومي الأمريكية أعداداً كبيرة من الأخصائيين في العلوم الرياضية وفي تحليل الشيفرة أكثر من أية منظمة خاصة أو وكالة حكومية (بالإضافة إلى كونها أكبر وكالة تشتري التجهيزات الحاسبية في العالم). يوجد أيضاً أخصائيون بتحليل الشيفرة يتم توظيفهم من قبل الشرطة وعدد قليل متناثر من وكالات تنفيذ القضاء ووكالات الاستخبارات الحكومية. افتراضياً جميع أعمال التشفير والبحث التي تنفذها الحكومة (باستثناء المؤسسة الوطنية للمعايير والتكنولوجيا) هي أعمال سرية ولا ترى ضوء النهار.
- **علمي أو مشترك.** حتى وقت قريب جداً، احتكرت الحكومة محللي الشيفرة وتحكمت بأعمالهم عموماً، لكن من جهة ثانية، تقلص تأثير الحكومة بشكل كبير نتيجة الاهتمام المتزايد بعلم التشفير من قبل أخصائيي العلوم الرياضية (والذين يقون في عالم التدريس)، ونتيجة الحاجة المتزايدة لمحللي الشيفرة من قبل الصناعات الخاصة وخاصة في القطاعات المالية، الاتصالات، وأمن الحواسب. هؤلاء الأخصائيون في تحليل الشيفرة منفتحون بصورة أكبر في عملهم، يلقون المحاضرات، وينشرون المقالات حول نقاط الضعف التي تعاني منها خوارزميات التشفير. وفي بعض الأحيان عندما يتم نشر إحدى نقاط الضعف،

يقوم المبرمجون الآخرون (ليس من الضروري أن يكونوا أخصائيين في تحليل الشيفرة) ببرمجة أدوات تستغل نقطة الضعف هذه. مثال تقليدي لهذا الأمر هو بروتوكول الأمن 802.11b Wired Equivalent Privacy (WEP)، إذ ظهرت عدة أدوات على شبكة الإنترنت، بعد وقت قصير من نشر المقالة العلمية التي تصف نقاط الضعف لهذا البروتوكول، والتي استطاعت كشف مفاتيح WEP. بالرغم من أن هؤلاء المبرمجين قد تنقصهم المهارات والخبرة لتحديد الخلل التقني في خوارزمية تشفير، إلا أنهم يتمتعون بالمهارات اللازمة للانتقال من مفهوم نظري إلى برنامج حقيقي.

في الحقيقة إنه من خارج نطاق هذا الكتاب التغلغل إلى تفاصيل تحليل الشيفرة وكيف يقوم الأخصائيون في تحليل الشيفرة بمعالجة البيانات المشفرة، ومع ذلك هناك بعض النقاط التي يجب أخذها بعين الاعتبار:

- يتطلب تحليل الشيفرة قدراً كبيراً من المهارات والمعرفة (وخاصة في العلوم الرياضية) وهذا أكثر مما يملكه الجاسوس العادي.
- هناك أخصائيون محترفون يقومون بإيجاد نقاط الضعف في أنظمة التشفير، وذلك إما مقابل المال، أو بدافع الفضول العلمي. وقد يكشف عملهم ضمنياً ما قد يعتقده العامة بأنه آمن.
- بالرغم من وجود أخصائيين أكثر موهبة في تحليل الشيفرة حالياً (وليسوا موظفين لدى الحكومة) والذين يتوقعون إمكانيات وكالة الأمن القومي الأمريكية والوكالات الأخرى التي تخترق الرموز والشيفرة، فلا تستخف أبداً بالمعارضة على مستوى الحكومة. تملك الحكومات كمية هائلة من الموارد تحت تصرفها، وهم على الأرجح متقدمون بعدة سنوات عن الدنيا العلمية والقطاع الخاص بخصوص التشفير.
- قد تحول الأبحاث الحديثة والمعالجات الأسرع أنظمة تشفير قوية إلى أنظمة ضعيفة، ومن المهم البقاء على تواصل بكل جديد في هذه المجالات في أيامنا هذه، وذلك بالاهتمام بموارد الأخبار الأمنية المطبوعة والإلكترونية. لا حاجة لئن تفزع عندما ترى عنواناً رئيساً عن أحد ما قد اكتشف نقطة ضعف في خوارزمية تشفير. حيث من وجهة نظر علمية قد تكون نقطة الضعف هذه موجودة، لكن في العالم الحقيقي لا تزال الخوارزمية آمنة، لأن الاستغلال الفعال ليس عملياً للاستفادة من ضعفه.



هناك عدد من المصادر على الإنترنت والتي تستكشف تحليل الشيفرة بتفصيل أكبر. ومنها الأسئلة التي تتكرر باستمرار لمخابر RSA حول التشفير اليوم (www.rsasecurity.com/rsalabs/faq/)، تحليل الشيفرة الأساسي (الكتيب

الخاص بالجيش 2-40-34 (/www.fas.org/irp/doddir/army/fm34-40-2)، ودورة تدريب ذاتي في تحليل الشيفرة الخاصة بالتعمية الكتلية (www.counterpane.com/crypanalysis.pdf).

أدوات الاختراق

والآن أنت جالس ويوجد حولك الكثير من المستندات التي خططت للحصول عليها من المشتبه به، وأنت تعلم بوجود أدوات تساعدك على اختراق هذه المستندات. كانت جدتك محاسبة رموز في الحرب العالمية الثانية وقد روت لك قصص حول علماء العلوم الرياضية ومخترقي الرموز الآخرين باستخدام القلم، الورقة، والحواسب البدائية لاختراق الرسائل المرمزة. لكنك اليوم لا تحتاج أن تكون خبيراً بتحليل الشيفرة لتكشف الأشكال العامة من البيانات المحمية. دعونا نستعرض بعض البرامج الخدمية، التجارية، المجانية، المؤتمتة، وسهلة الاستخدام، والتي تتحايل بسهولة على أمن الملفات المشفرة.

تطبيقات اختراق كلمات المرور

يعتبر اختراق كلمات المرور سوقاً محدوداً واختصاصياً نوعاً ما، وهناك مجموعة من الشركات التي تصمم برمجيات لكشف كلمات المرور. يتم ذلك عن طريق تطبيق مبدأ الهندسة العكسية على التطبيقات التي تولد المستندات المحمية لفهم نوع خوارزمية التشفير المستخدمة، وبناءً على هذه المعلومات يكتب المبرمج شيفرة لبرنامج خدمي يقوم إما بخرق التشفير الضعيف ويكشف كلمة المرور أو يقوم بمهاجمة القاموس أو مهاجمة القوة العمياء على الملف المحمي.

يوجد تقريباً لكل تطبيق برمجي معروف يستخدم كلمة مرور لحماية البيانات أداة مطابقة تقوم بإلغاء حماية البيانات. يمكن كشف كلمة المرور، بحسب طريقة تشفيرها، مباشرة أو قد تستغرق أيام وأسابيع لكشفها. ليكون لديك فكرة عن مدى سهولة اختراق المستندات المحمية، فيما يلي لائحة بأنواع الملفات والمنتجات التي يستطيع برنامج ElcomSoft، أحد رواد استرداد كلمات المرور، أن يخترقها:

- برنامج Adobe Acrobat: ملفات ذات اللاحقة PDF.
- برمجيات الضغط: ملفات ذات اللاحقة Zip، RAR، ACE، وARJ.
- منتجات شركة Corel: وتتضمن البرامج WordPerfect، QuattroPro، وParadox.

- برامج البريد الإلكتروني: Microsoft Internet Mail and News، Eudora، TheBat!، Netscape Navigator، Communicator Mail، Pegasus، Calypso، FoxMail، IncreditMail، @nyMail، و QuickMAil Pro.
- برامج المراسلة الفورية Instant Messengers: ICQ، Yahoo، AOL Aim، Msn Messenger، Excite Messenger، Odigo، Trillian، AT&T IM Anywhere، T-Online Messenger، Match Messenger، Praize IM، ScreenFIRE، ACD Express Communicator، Imici Messenger، Prodigy IM، PowWow Messenger، Jabber IM، Kellster IM، PalTalk، Indiatimes Messenger، Miranda، وTiscali.
- منتجات شركة Intuit: Quicken، Quicken Lawyer، وQuickBooks.
- منتجات شركة Lotus: SmartSuite، Organizer، WordPro، 1-2-3، وApproach.
- منتجات شركة Microsoft: البرامج المكتبية Access، Excel، Outlook، Word، Outlook Express، Internet Explorer، Project، Money، Backup، وVisual Basic للتطبيقات.
- منتجات Symantec ACT.

ربما سوف تشعر يا قارئي الكريم ببعض الغضب، وتتساءل كيف يمكن للشركات أن تنشر برمجيات التجسس. تذكر أنه مثل أية تقنية أخرى يمكن استخدام برامج الاختراق بصورة قانونية وغير قانونية. من أحد الجوانب الإيجابية مثلاً يستطيع المستخدم بواسطة هذه البرامج استرداد المستندات المحمية عند نسيان كلمة المرور، استبدالها عن طريق الخطأ، أو ضياعها. كما تساعد هذه الأدوات أيضاً في اكتشاف الدليل أثناء التحقيقات الجنائية (تمثل وكالات القانون زبوناً جيداً لهذه الشركات).

تنص قاعدة الإبهام لبرمجيات الاختراق على أنه كلما كان المعالج أسرع كلما تم إنجاز مهاجمة القاموس أو مهاجمة القوة العمياء بشكل أسرع، ترتبط السرعة المقاسة بواحدة MHz بشكل مباشر بعدد كلمات المرور التي يجربها البرنامج كل ثانية، كلما زادت السرعة، زاد عدد المحاولات في الثانية.

تعمل جميع تطبيقات اختراق كلمات المرور في الخلف، أثناء قيامك بأعمال أخرى، لكن كلما زاد عدد العمليات التي تقوم بتشغيلها كلما أثقل المعالج بتطبيقات أخرى، وبالتالي سيكون تطبيق الاختراق أبطأ. تتضمن بعض تطبيقات الاختراق إعدادات تمكنك من تثبيت أولوية التطبيق لضمان حصول البرنامج على أكبر قدر ممكن من دورات المعالج الممكنة، لكن الخيار الأفضل هو تكريس حاسباً أو أكثر للقيام بالاختراق.

غالباً ما تقوم شركات اختراق كلمات المرور بتحديث منتجاتها، وذلك بزيادة سرعة وفعالية البرنامج الخدمي، وتوجيه طرق جديدة للحماية والتشفير المستخدمة من قبل مصنعي البرمجيات. إلى جانب شركات برمجيات استرداد كلمات المرور، توجد شركات خدمية تقوم بإلغاء حماية المستندات التي ترسلها للشركة. إن معظم برمجيات الاسترداد التجارية غير مكلفة، ومن المفيد أن يضع المرء هذه البرمجيات تحت تصرفه.

تناقش في الفقرات التالية بعض المساهمين الأساسيين في العمل التجاري المتعلق باختراق كلمات المرور.

وسائل التجارة: اختراق المكونات الصلبة

يوجد خيار آخر للحكومات وعمليات التجسس الممولة جيداً وهو التجهيزات الصلبة المكرسة والمصممة خصيصاً لاختراق البيانات المشفرة.

بالرغم من أن "تجهيزات صلبة مكرسة" يبدو غريباً بعض الشيء ويمكن أن يتواجد فقط في وكالة الأمن القومي الأمريكية، إلا أنه في عام 1998 بنت مؤسسة الرواد الإلكترونيين Electronic Frontier Foundation (EFF) حاسباً مصمم خصيصاً لاختراق البيانات المشفرة باستخدام خوارزمية التشفير DES. تكونت الآلة من 1,500 رقاقة، واحتوى كل منها على 24 محرك بحث متماثل قادر أن يجرب مليونين ونصف المليون كلمة مرور في الثانية. وقد استطاع مخترق خوارزمية DES بشكل صاعق اختبار تسعين مليار مفتاح في الثانية، وهذا سيستغرق تسعة أيام فقط لإنجاز بحثاً شاملاً لجميع التركيبات الممكنة (غالباً يشار إليها بفضاء العنوان).

لقد استطاعت الآلة، عند الظهور الرسمي الأول لها، اختراق رسالة مشفرة باستخدام مفتاح طوله 56 بت في أقل من 56 ساعة (وفي نفس الوقت، كان الرقم القياسي السابق، الذي استخدم مهاجمة موزعة قد بلغ 39 يوماً). وفي النهاية تم تحطيم هذا الرقم القياسي باستخدام المكونات الصلبة للاختراق بالتعاون مع جهود الاختراق الموزعة. لقد تم اكتشاف المفتاح الصحيح، باختبار أكثر من 245 مليار مفتاح في الثانية، خلال 22 ساعة أو أكثر بقليل. (لمعلومات مفصلة عن مخترق خوارزمية DES التابع لمؤسسة الرواد الإلكترونيين EFF، بما فيها الصور، اتبع الرابط www.cryptography.com/resources/whitepapers/DES.html).

لاحظ أنه إذا كان بمقدور مجموعة تأييد لا ربحية بناء جهاز اختراق ذو تقنية منخفضة لكنها فعالة مقابل أقل من 250,000 دولار أمريكي، فبالتأكيد أن وكالات الاستخبارات الحكومية ووكالات القضاء يملكون مثل هذه الأجهزة تحت تصرفهم.

هل من الممكن تطوير تجهيزات متخصصة لإنجاز نفس العمل مع أنظمة تشفير أقوى، مثل معيار التشفير المتقدم Advanced Encryption Standard (AES)[1] والذي يستخدم مفتاحاً يبلغ طوله 128 بت؟.

لنفترض أنه بمقدورك استخدام طاقة حاسبية كافية لبناء آلة تستطيع استرداد مفتاح DES يبلغ طوله 56 بت في ثانية واحدة، حتى مع كل تلك القدرة الحصانية سيستغرق الأمر 149 تريليون سنة لإنجاز بحث شامل عبر جميع المفاتيح الممكنة ذات طول 128 بت. في الواقع هذا وقت طويل على ما أظن وخاصة أن معظم العلماء يعتقدون أن عمر الكون أقل من 20 مليار سنة.

ACCESSDATA: تأسست شركة AccessData عام 1987، وهي إحدى الشركات الرائدة المتخصصة باسترداد كلمات المرور. لقد زودت الشركة خدمات استشارية وبرمجيات للحكومة الأمريكية، وكالات القانون الفدرالية والمحلية، وشركة America المتحدة، وكنتيجة لهذا تتمتع الشركة بسمعة طيبة بين الزبائن. تتراوح كلفة وحدات اختراق كلمات المرور لعدد من التطبيقات الشهيرة من 35 إلى 99 دولار أمريكي، وتباع جميع هذه الوحدات معاً بسعر 495 دولار أمريكي بصفتها مجموعة الأدوات لاسترداد كلمة المرور.

يوجد لدى شركة AccessData أيضاً منتج يسمى Distributed Network Attack (DNA) لاختراق المستندات المكتبية الخاصة بشركة Microsoft الإصدار 97/2000 وملفات PDF.. يتضمن البرنامج DNA ملقماً مركزياً وعدداً من عملاء الشبكة بحيث تتحقق كل مجموعة من العملاء من مجموعة محددة من كلمات المرور المحتملة، وهكذا يتناقص مقدار الوقت الكلي لإنجاز البحث الشامل. تبلغ كلفة الإصدار ذا العشر عملاء 249 دولاراً أمريكياً، والإصدار ذا المائة عميل 995 دولاراً أمريكياً.

لمزيد من المعلومات، ولتحميل إصدار تجريبي لمجموعة الأدوات لاسترداد كلمة المرور، اتبع الرابط www.accessdata.com.

ELCOMSOFT: وهي شركة برمجيات روسية مثيرة للجدل متخصصة في برمجيات استرداد كلمات المرور، أطلقت الشركة برنامجها الأول لاختراق كلمات المرور للملفات المضغوطة المحمية عام 1997، ومنذ ذلك الوقت طورت عدداً من برامج الاختراق لكثير من التطبيقات المعروفة، تتراوح أسعار البرامج الفردية من 30 إلى 79 دولاراً أمريكياً مقابل تراخيص نظامية.

عرفت شركة ElcomSoft بشكل واسع في مجالات الحقوق الرقمية ودورات أمن الحواسب خلال صيف عام 2001، وذلك عندما تم اعتقال أحد موظفي الشركة Dmitry Sklyarov خلال

[1] AES هي خوارزمية تشفير معتمدة من قبل وكالات حكومة الولايات المتحدة لاستخدامها في تشفير المستندات الحساسة، وقد تم اعتماد هذا المعيار بدلاً من معيار *DES* القديم. تعتبر *AES* خوارزمية تشفير بمفتاح متناظر، وهي تدعم أطوالاً للمفاتيح تصل إلى 256 بت.

مؤتمر المخربين المنعقد في Las Vegas، وذلك بعد إلقائه عرضاً تقديمياً شرح من خلاله ضعف التشفير الذي تستخدمه شركة Adobe لحماية الكتب الإلكترونية. وقد طور Sklyarov منتجاً لشركة ElcomSoft يقوم بفك تشفير الكتب الإلكترونية من شركة Adobe، من جهتها ضغطت شركة Adobe على الحكومة لاعتقال Sklyarov بتهم انتهاك قرار حقوق النشر الرقمي في الألفية Digital Millennium Copyright Act (DMCA).

قضى Sklyarov عدة أسابيع في السجن قبل أن يتم إطلاق سراحه بكفالة بلغت قيمة 50,000 دولار أمريكي وفي النهاية سمح له بالعودة إلى روسيا. (وقد صرح Alexander Katalov، رئيس شركة ElcomSoft والذي كان عميلاً سابقاً للمخابرات الروسية KGB، في وقت لاحق أنه كان أمراً مثيراً للسخرية قيام مكتب التحقيقات الفدرالي باعتقال Sklyarov، مع العلم بأن وكالة القانون الفدرالية كانت من أحد زبائنه). بالرغم من إسقاط التهم الموجهة ضد Sklyarov، قررت الحكومة مع ذلك ملاحقة الشركة على نفس الأسس، إلا أن هيئة المحلفين برأت الشركة في شهر كانون الأول (ديسمبر) عام 2002. (أما شركة Adobe، والتي كانت غير جادة في دعمها للمقاضاة. فقد خرجت من الصورة بهدوء، بالصدفة عندما هددت عدة جماعات من الناشطين بتنظيم إضراب لمنتجات الشركة).

لم تقف شركة ElcomSoft، بعد هذا الحادث حيث أصبحت ضحية تجريب القرار DMCA، وقامت بإصدار عدد من المنتجات المبتكرة لاختراق كلمات المرور. يمكنك الحصول على مزيد من المعلومات وتحميل إصدار تجريبي من الرابط www.elcomsoft.com .

PASSWARE: وهي شركة أوروبية أخرى جديدة صعدت بسرعة وأصبحت من أوائل باعة منتجات اختراق كلمات المرور. تأسست الشركة في أستونيا عام 1998 (لقد خلف الاتحاد السوفييتي السابق بعض المبرمجين الأذكياء ذوي ميل إلى أمن الحواسب)، تقدم الشركة برامج خدمية للاختراق لعدد من التطبيقات المعروفة، والمتوفرة فردياً ومسعّرة من القيمة 45 إلى 195 دولاراً أمريكياً، أو مجتمعة مع بعضها تحت اسم مجموعة الأدوات PassWare مقابل 395 دولاراً أمريكياً. يبين الشكل 1-6 أحد برامج اختراق كلمة المرور. لتحميل إصدار تجريبي ولمزيد من المعلومات اتبع الرابط www.lost-password.com.

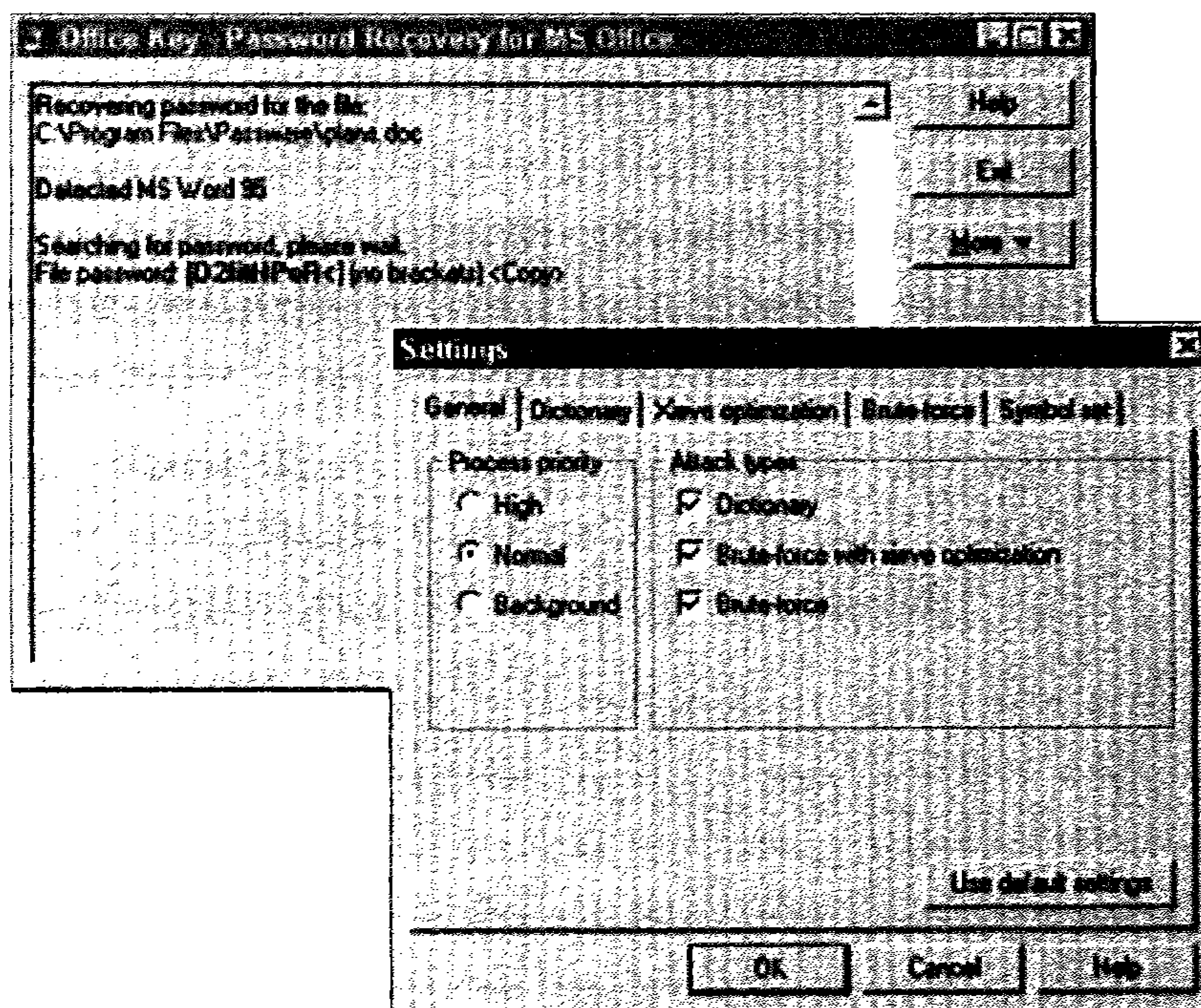
برامج اختراق أخرى: إلى جانب البرامج المنتجة من قبل هذه الشركات الثلاثة، يوجد أيضاً عدد من البرامج التجارية المجانية والتي تستطيع كشف المستندات المحمية باستخدام كلمة مرور. تعمل بعض هذه الأدوات المجانية بصورة جيدة كمثيلاتها من البرامج التجارية في مجال الاسترداد. وفيما يلي بعض الموارد التي يمكنك التحقق منها:

- يمثل موقع Pavel Semjanov "Russian Password Crackers"، أحد أفضل المصادر الشاملة لبرامج الاختراق. يملك Semjanov لائحة شاملة لبرامج كلمات المرور التجارية والمجانية،

مع وجـــود وصف مختصـــر وتعليقـــات حول مـــدى فعالـــية البرنـــامج. اتبع الرابـــط .www.password-crackers.com

- يشكـــل موقع Joe Peschel "D.O.E SysWorks"، مصدر آخر جيد للمعلومـــات حول المخربيـــن، التشفيـــر الضعيف، ومواضيـــع تتعـــلق بالأمـــن العـــام، علـــى الرابـــط .http://members.aol.com/jpeschel/

- وأخيراً، يمكن تحميل عدد من برامج اختراق كلمات المرور لأنظمة التشغيل المختلفة والتطبيقات من موقع الويب Packetstorm security المحترم، www.packetstormsecurity.org/assess.html.



الشكل (6-1) اختراق برنامج لشركة Passware لمستند محمي بكلمة مرور تم إنشاؤه من قبل إصدار قديم من البرنامج Microsoft Word 95 (من مشهد المجرم المشتبه به في بداية هذا الفصل) في أقل من ثانية. كانت كلمة المرور >D2fitHPoR. يستغرق اختراق المستندات التي تم إنشائها وحمايتها باستخدام إصدارات أحدث من برنامج Microsoft Word زمناً أطول لكنها ما تزال معرضة للاختراق. اتبع الرابط http://support.microsoft.com/default.aspx?scid=KB;en-us;q290112 للحصول على معلومات مفصلة عن خوارزميات التشفير التي تستخدمها شركة Microsoft.

اختراق التشكيلات الجانبية PWL. لأنظمة التشغيل WINDOWS 3.X.9X.ME

لا تقدم عائلة أنظمة التشغيل Microsoft Windows 3.x/9x/ME الكثير في مجال أمن نظام التشغيل، كما رأينا في الفصل الرابع. لا يحد مربع حوار تسجيل الدخول الوصول إلى الحاسب لأنه يمكنك ببساطة ضغط زر إلغاء الأمر وسيتم تحميل النظام Windows وعرض سطح المكتب، ويمنحك الوصول الكامل إلى جميع الملفات على القرص الصلب.

كل ما يقوم به تسلسل تسجيل الدخول هو تغيير إعدادات العرض اعتماداً على اسم المستخدم ويستعيد الوصول إلى الأدلة المشتركة، أرتال الطباعة، ومشاركات الشبكة. لتسهيل هذه العملية، بدلاً من إدخال كلمة المرور كل مرة ضمن صندوق الحوار للوصول إلى هذه الموارد، يتم الاحتفاظ بقائمة من كلمات المرور المشفرة ضمن ملف ذو اللاحقة PWL.، ومن ثم يتم فك تشفيرها عن طريق كلمة المرور عند تسجيل الدخول.

الهدف الأساسي من مهاجمة التشكيل الجانبي هو كشف أي كلمات المرور من الممكن أن تكون مخزنة في الملف، فقط في حالة كون كلمات المرور هذه تحمي ملفات أخرى. بعد الحصول على هذه المعلومات فمن الجدير نسخ أي ملفات ذات اللاحقة PWL. التي كانت موجودة على الحاسب المحمول الخاص بالمشتبه به، ومن ثم مهاجمة هذه الملفات في مكان آمن.

أعتقد أنه من الهام معرفة القليل عن تاريخ مخططات التشفير التي استخدمتها شركة Microsoft لأنها تتباين تبعاً لنظام التشغيل المستخدم.

- نظام التشغيل Windows for Workgroups (3.11) ونظام التشغيل Windows 95، تم استخدام تنفيذ ضعيف جداً لخوارزمية التشفير RC4، حيث تتمكن البرامج المجانية مثل Glide ببساطة وبسرعة كشف أي كلمات مرور مخزنة.
- وجهت شركة Microsoft هذا الخلل الأمني إلى الإصدار OSR2 لنظام التشغيل Windows 95 وطبقت الإصلاح على الأنظمة Windows 98/ME. لا تستطيع البرامج مثل Glide وبرامج الجيل الأول من PWL عرض كلمات المرور لهذه الأنظمة اللاحقة، لكن لا تزال هناك طريقتان لشن الهجوم، حيث يتم تخزين جميع كلمات المرور الموجودة ضمن الملف PWL.، في الذاكرة المخبئية على شكل نص صريح غير مشفر، فإذا كان الحاسب الهدف في حالة عمل، يمكنك تنفيذ أداة مثل PWLView لعرض جميع كلمات المرور. أما إذا كان الحاسب الهدف مطفئاً، فقم ببساطة بإقلاعه وانسخ ملفات PWL. إلى قرص مرن ومن ثم استخدم أداة مثل PWLHack أو PWLTool لشن مهاجمة القوة العمياء أو مهاجمة القاموس على الملف.

تتوفر أدوات اختراق ملفات PWL. عبر عدد من مواقع الويب المتعلقة بالأمن والاختراق، يمكنك تحميل أكثر الأدوات فعالية وانتشاراً من الروابط التالية:

- **Glide**: أداة مجانية، http://members.aol.com/jpeschel/Glidepwl.zip.
- **PWLView**: أداة مجانية، http://lastbit.com/vitas/pwlview.asp (تتوفر نسخة تجريبية)
- **PWLTool**: تكلفتها 40 دولار أمريكي، يمكنك تحميل النسخة التجريبية من http://lastbit.com/vitas/pwltool.asp.
- **PWLHack**: أداة مجانية تتوفر على الرابط:

www.pilabs.org.ua/wisdom/download/pwlhack/pwl_h410.rar.

اختراق مربع حوار كلمة المرور

طريقة أخرى لكشف كلمات المرور تم استخدامها لأغراض متعددة هي استخدام برنامج رؤية الأشعة السينية على مربعات الحوار. يتمتع نظام التشغيل Windows بميزة أمنية وهي استبدال نص كلمة المرور التي يتم إدخالها في مربع الحوار برمز النجمة (*). تمنع هذه الخاصية شخصاً يقف بجانبك من معرفة كلمة المرور.

يستطيع المبرمج في التطبيقات التي تتمتع بهذه الميزة، تطبيق نموذج التحكم بالتحرير على ES_PASSWORD، وعندما يطبع المستخدم كلمة المرور ضمن التحكم بالتحرير يظهر النص على شكل رموز النجمة، لكن بما أن النص الصريح لا يزال مخزناً في الذاكرة، فمن الممكن استرجاع النص بالوصول إلى مقبض التحكم (مرجع إلى الذاكرة).

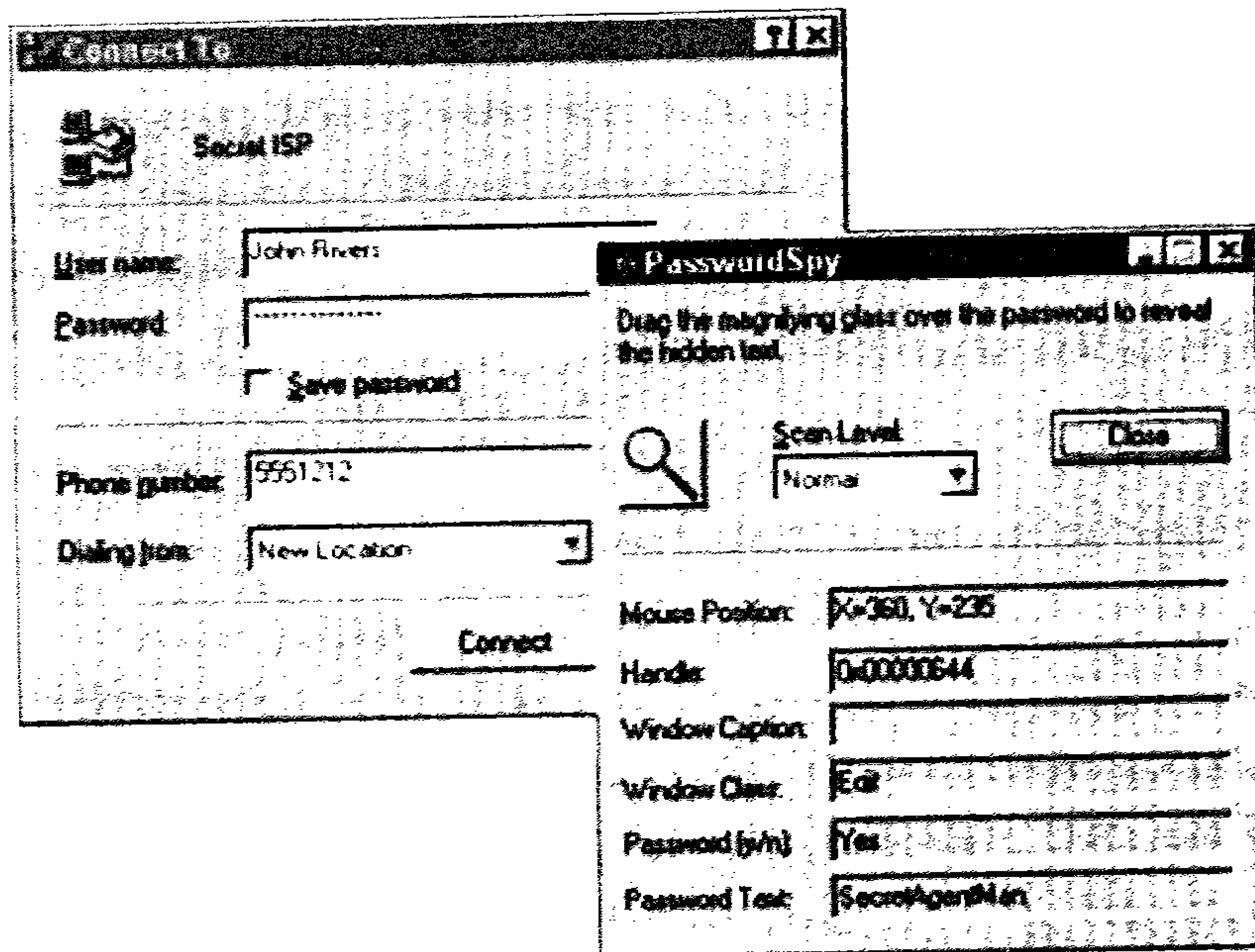
تستخدم الكثير من التطبيقات التي تستخدم كلمات المرور هذه الميزة، مثلاً يسمح برنامج WS_FTP للمستخدمين أن يحفظوا كلمات المرور المرتبطة بحسابات FTP لتجنب إدخال البيانات في كل مرة يقومون فيها بعملية تسجيل الدخول، يُظهر مربع حوار الحاسب المضيف، اسم الحساب، وكلمة المرور (المعروضة على شكل رموز النجمة).

تستطيع الأدوات المجانية مثل Revelation و Snitch الوصول إلى نص كلمة المرور المخفي وإظهار ما تحت رمز النجمة بسرعة، مثل البطل Super Man الذي يتمتع برؤية الأشعة السينية، ما عليك فعله هو تشغيل البرنامج وتمرير مؤشر الفأرة على رموز النجمة، وبسرعة تظهر أمامك كلمة المرور.

غيرت شركة Microsoft في أنظمة التشغيل Windows 2000/XP الطريقة التي يتم بها التحكم بتحرير كلمة المرور، وبالتالي لم تعد تصلح البرامج التي نجحت في أنظمة التشغيل السابقة

لكشف كلمات المرور في الإصدارات الحديثة. هناك أداتان تصلحان لجميع إصدارات نظام التشغيل Windows وهما الأداة التجارية iOpus Password Recovery XP، والأداة المجانية المفتوحة المصدر PasswordSpy، كما في الشكل 6-2.

لا تنجح طريقة اختراق مربع حوار كلمة المرور مع جميع التطبيقات (يدرك بعض مطورو التطبيقات هذا الأمر ويكتبون شيفرة خاصة لمنع استغلال نقطة الضعف هذه)، لكنها مع ذلك طريقة سهلة وسريعة لكشف كلمات المرور التي يمكن استخدامها في مكان آخر لحماية البيانات في التطبيق التي تعمل عليه.



الشكل (6-2) يكشف البرنامج PasswordSpy كلمة مرور محمية في مربع الطلب الهاتفي للشبكة لنظام التشغيل Windows 98.

فيما يلي بعض الأدوات الشائعة لاختراق مربع حوار كلمة المرور:

- Revelation: أداة مجانية، www.snadboy.com.
- Snitch: أداة مجانية، http://ntsecurity.nu/toolbox/snitch.
- iOpus Password Recovery XP: تبلغ تكلفتها 29.95 دولار أمريكي، www.iopus.com/password_recovery.htm (تتوفر نسخة تجريبية للأداة).

- PasswordSpy: أداة مجانية، www.csc.calpoly.edu/~bfriesen/software/pwdspy.shtml (مع الشيفرة)

اختراق شبكة الطلب الهاتفي

هناك مكان آخر حيث يمكنك كشف كلمات المرور الضعيفة، وهو شبكة الطلب الهاتفي في نظام التشغيل Windows (Dial-Up Networking (DUN)). تسمح هذه الخدمة بقيام المستخدمين بتعيين كلمات المرور بسهولة لمزودات خدمة الإنترنت وخدمات الشبكة الأخرى، ومن إحدى الميزات الظريفة لشبكة الطلب الهاتفي DUN هي وجود خيار لحفظ كلمة المرور وذلك ليتذكر النظام كلمة المرور في كل مرة تقوم بها بالاتصال باستخدام حساب ما دون الحاجة إلى إعادة إدخال المعلومات الخاصة بهذا الحساب. تكون شبكة الطلب الهاتفي غير محمية بشكل خاص في أنظمة التشغيل Windows 9x/ME، كما تتوفر عدة أدوات سطر الأوامر يمكنها اختراق الحساب ذو التشفير الضعيف ومعلومات كلمة المرور، ومن هذه الأدوات ما يلي:

- Dialpwd: أداة مجانية، www.password-crackers.com/DOWNLOAD/dialpwd.zip.
- PhoneBook Viewer v1.01dc: أداة مجانية، www.password-crackers.com/DOWNLOAD/phbv101c.zip

اختراق أنظمة التشفير

إن اختراق المستندات المحمية ليس بالعملية الصعبة، لكن ماذا لو كان الهدف يستخدم برمجيات تشفير قوية؟ في هذه الحال قد تواجهك بعض الصعوبات، ما لم يحالفك الحظ، لتكشف البيانات المحمية الخاصة بالهدف، بالإضافة إلى أن أنظمة التشفير الحديثة مثل PGP، Blowfish Advanced CS (وغيرها من الأدوات التي تمت مناقشتها في فقرة "الإجراءات المضادة" من الفصل الخامس) تتمتع بمقاومة عالية ضد المهاجمات التي تنجح في التطبيقات ذات التشفير الضعيف.

من المستحيل حالياً إجراء مهاجمة القوة العمياء بصورة شاملة على البيانات المشفرة باستخدام خوارزمية تشفير قوية ومفتاح بطول ملائم، لكن من الممكن جداً إجراء مهاجمة قاموس أو مهاجمة قوة عمياء محدودة على أمل أن الهدف قد استخدم كلمة مرور ضعيفة. هناك أيضاً أدوات لمهاجمة القاموس ومهاجمة القوة العمياء والتي تكون فعالة ضد بعض خوارزميات التشفير الشائعة، لكنها غير متوفرة بمتناول اليد مثل البرامج التي تخترق كلمات المرور للتطبيقات، إذا كنت تميل إلى الأمور التقنية ربما ستحاول أن تبرمج أداتك الخاصة لاختراق أي خوارزمية تشفير تم استخدامها لحماية البيانات. (أو في حالة الجاسوس الحكومي الافتراضي الذي نستخدمه كمثال، يمكنك تسليم هذه البيانات لمجموعة من المحللين التقنيين ليحاولوا اختراق البيانات).

إحدى مشاكل اختراق البيانات المشفرة تشفيراً قوياً هي أنك لا تعرف ما هي خوارزمية التشفير التي تم استخدامها لحماية البيانات. تترك بعض البرامج مثل PGP ترويسة في الرسالة المشفرة والتي تحدد مباشرة التطبيق الذي تم استخدامه لحماية المعلومات، لكن أنظمة التشفير الأخرى لا تعطيك أدنى فكرة عن هذا. إن عدم معرفة فيما إذا كانت البيانات محمية باستخدام الخوارزميات IDEA، 3DES، Blowfish أو أي عدد من الخوارزميات الأخرى، يعرقل مهاجمات القاموس والقوة العمياء إعاقة شديدة، لذلك يجب عليك دائماً أن تبحث عن أي أدوات تشفير قد تكون موجودة على القرص الصلب أو وسائط التخزين الأخرى. والآن مع توفر هذه المعلومات ومع توفر محرك بحث، تستطيع إيجاد نقاط الضعف المعلن عنها المرتبطة بالأداة أو البرامج التي تساعدك على كشف البيانات المحمية باستخدامها.

الأمر الجيد هو قلة الذين يستخدمون التشفير القوي، وإذا واجهتك بيانات محمية والتي من الصعب كشفها باستخدام برنامج تشفير، يمكنك في هذه الحالة إتباع بعض الخيارات الأخرى. حيث من الأسهل والأسرع استخدام برنامج مسجل المفاتيح، كاميرا للمراقبة، أو تطبيق حصان طروادة للحصول على البيانات المطلوبة.

الإجراءات المضادة

فجأة قررت ترك عملك، لأن العمل الخاص يدفع لك راتباً أفضل من خدمة التجسس العام (كما أنه أقل خطراً)، والآن حصلت على وظيفة مربحة بعملك في شركة Fortune 500 على أمن الحواسب. من أحد مسئولياتك حماية البيانات البالغة الدقة للشركة من مهاجمات الجواسيس، وخاصة فيما يتعلق بالتجسس الاقتصادي.

دعونا الآن نراجع بعض الإجراءات المضادة البسيطة وغير المكلفة والتي تعتمد على التشفير القوي وكلمات المرور القوية والتي سوف تستخدمها كجزء من خطتك لمنع الجواسيس من الوصول إلى البيانات الحرجة.

التشفير القوي

وهو ليس أمراً فائق الذكاء، إذا كنت تملك بيانات تريد حمايتها، فلا تتكل على ميزات الحماية باستخدام كلمات المرور الموجودة في الكثير من الحزم البرمجية التجارية. إنما يجب عليك استخدام الملف القوي وتطبيقات التشفير الآنية، التي ناقشناها في الفصل الخامس. لكن لا تخدع نفسك بقوة خوارزمية التشفير التي تستخدمها، حيث كما رأيت سابقاً من خلال الكتاب، توجد طرق كثيرة لتشفير المعلومات.

حسن إدارة كلمات المرور

قد تعتقد أن التجسس الحاسي يتعلق بمواضيع مثيرة للاهتمام – وليس بسياسات بيروقراطية مملة، لكن السياسات الأمنية الجيدة هي إجراء أساسي ضد محاولات التجسس، سياسة كلمة المرور هامة جداً لأن كلمات المرور نقطة ضعف يمكن أن يستغلها الجاسوس بسهولة.

ليس من الضروري أن تملك مؤسسة ضخمة لتكوّن سياساتك الأمنية الخاصة، حتى من غير الضروري أن تكتب السياسة (مع أنها فكرة جيدة لتتمكن من تذكرها أو تشاركها مع الأشخاص الآخرين إذا كنت تعمل لصالح منظمة). سوف يعطيك هذا القسم بعض الأفكار لتكوّن سياسة كلمة المرور الخاصة بك.

تذكر أن مفتاح حسن الإدارة الناجحة هو الامتثال للأوامر، فإذا لم تقم بإتباع السياسة بدقة، فسوف تعرّض نفسك للمهاجمات التي قد تكشف البيانات.

كلمات المرور "القوية"

لا بد أنك قد عرفت ما هي كلمات المرور القوية، فهي بالتأكيد لن تكون اسم زوجتك، تاريخ ميلادك، كلمة من كلمات القاموس، اسم حسابك، أو كلمات المرور الضعيفة الأخرى والتي يمكن أن تتعرض للهجوم ببساطة. وفيما يلي مواصفات كلمة المرور القوية:

- يبلغ طولها ثمانية محارف على الأقل (كلما كانت أكثر كان هذا أفضل، وخاصة إذا كنت تواجه خصماً يمتلك موارد ضخمة).
- ليست كلمة (في أي لغة من اللغات).
- ليست معتمدة على معلومات شخصية.
- تتضمن محارف كبيرة وصغيرة (مثلاً، a-z وA-Z).
- تتضمن أرقاماً وعلامات ترقيم بالإضافة إلى الأحرف (مثلاً، 0-9 وأي مما يلي: (!@#$%^&*()_+|~- -=\{}[]:":'< >?[]./).
- من السهل تذكرها، أي لست بحاجة إلى كتابتها.
- لا يتم كتابتها أو حفظها إلكترونياً أبداً ما لم تشفر.

من أحد أفضل الطرق لاختيار كلمات المرور القوية هي استخدام ما يسمى passphase (عبارة مرور)، وهي عبارة عن سلسلة من الكلمات و/أو المحارف والتي تشكل عبارة لا تنسى – مثلاً،

Mycat$Is1Fatty أو *Iht1tAM (I hate traffic in the AM). عبارات المرور مقاومة بشكل كبير لمهاجمات القوة العمياء، بسبب طولها غير المحدد ومزيج المحارف.

لكن كلمة المرور القوية جيدة بمقدر جودة خوارزمية التشفير المستخدمة معها. حيث استخدم المجرم الافتراضي الذي نتعامل معه كلمة مرور قوية لكنها يمكن أن تكشف مباشرة إذا قام باستخدامها لحماية مستند يستخدم نسخة قديمة من محرر النصوص Word، والذي يتصف بتشفير ضعيف جداً.

كلمات المرور التي يتم توليدها عشوائيا

ينصح بعض خبراء الأمن زبائنهم باستخدام كلمات المرور التي يتم توليدها عشوائياً: اختيار تسلسل أحرف، أرقام، ورموز شبه عشوائي (تذكر، من الصعب الوصول إلى العشوائية البحتة). والسبب هو أن ذلك يمنع المستخدمين من اختيار كلمات المرور الضعيفة، وهذا ما يميل إليه معظم المستخدمين. بإمكانك استخدام أي محرك بحث لإيجاد عدد من البرامج الخدمية المجانية التي تولد كلمات مرور عشوائية.

مع أن هذه الطريقة تبدو معقولة، إلا أن الدراسات تشير إلى أن هذا الأسلوب قد يعاني من الأخطاء. يعاني المستخدم من صعوبة تذكر كلمات المرور التي يتم توليدها عشوائياً، وهي قوية بنفس القدر الذي تكون فيه كلمات المرور المعتمدة على عبارة سهلة التذكر في اختبارات مختلفة. إذا كنت من مستخدمي كلمات المرور التي يتم توليدها عشوائياً، فإنه تفوق التكاليف المرتبطة بتوليدها وتذكرها الفوائد الأمنية التي يتم إدراكها.



يمكنك الإطلاع على مقالة ممتازة بعنوان "The Memorability and Security of Passwords – Some Empirical Results." مكتوبة من قبل Jianxin Yan، Alan Blackwell، Ross Anderson، و Alasdair Grant. تكشف هذه المقالة فكرة أن كلمات المرور العشوائية هي الأعلى كما تقدم أو تعرض معلومات مثيرة أخرى حول استخدام كلمات المرور. يمكنك الحصول على المقالة من خلال الرابط www.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf.

استخدام كلمة المرور

تذكر دوماً أن كلمة المرور مثل البيت المصنوع من أوراق اللعب (أو الدومينو، تفاعل متسلسل، تأثير متموج، أو أي كناية قد تجدها مناسبة). إذا استخدمت نفس كلمة المرور القوية لكل شيء وتم كشفها بطريقة ما، يمكنك بعدها توديع جميع بياناتك المحمية.

واحدة من طرق تقليل عدد كلمات المرور التي عليك أن تتذكرها هي التصرف مثل وكالات الاستخبارات الحكومية واستخدام كلمات المرور المصنّفة. حيث يمكنك استخدام عدة كلمات مرور لمعلومات ونشاطات مختلفة. فعلى سبيل المثال، يعتبر إرسال رسائل مشفرة إلى المحامي نشاط ذو سرية عالية، أما تسجيل الدخول إلى منتديات تسلية متنوعة فهو نشاط ذو سرية منخفضة، فإذا تم كشف كلمة المرور الخاصة بالنشاط الثانوي، فهذا لن يؤثر على نشاطاتك السرية والهامة.

الحماية باستخدام مبدأ الهندسة الاجتماعية

كما ذكرنا سابقاً، يحاول الجاسوس المحترف أن يستغل نقاط الضعف التقنية والبشرية بهدف مهاجمة النظام الأمني. وفي كثير من الحالات، من الممكن الحصول على كلمة المرور بشكل أكثر فعالية وكفاءة باستخدام طرق الهندسة الاجتماعية والتي تستند على طبيعة الشخص وتصرفاته. يجب أن تدمج سياسة كلمة المرور الخاصة بك أساليب الحماية التالية ضد مهاجمات الهندسة الاجتماعية:

- لا تكشف كلمة المرور عبر الهاتف إلى أي شخص.
- لا تكشف كلمة المرور عبر البريد لإلكتروني.
- لا تكشف كلمة المرور إلى مديرك أو زملائك في العمل.
- لا تذكر كلمة المرور أمام أشخاص آخرين.
- لا تذكر موضوع كلمة المرور، مثل "اسم زوجتي".
- لا تكشف كلمة المرور في استطلاعات الرأي في المنتديات.
- لا تشارك كلمة المرور مع أفراد العائلة.
- لا تستخدم التلميحات السهلة لكلمة المرور في التطبيقات أو مواقع الويب التي تمنحك الوصول في حال نسيت كلمة المرور. حيث تسهّل هذه التلميحات الاحتمالات المتوقعة للجاسوس ليكشف حساب البريد الإلكتروني.
- لا تستخدم نفس كلمة المرور لحماية المعلومات الحساسة والهامة والتي قد تدخلها في موقع ويب.

تغيير كلمات المرور بانتظام

كلما طالت مدة استخدامك لنفس كلمة المرور، كلما زادت فرص كشفها بالصدفة أو بشكل متعمد. لذلك يتوجب عليك تغيير كلمة المرور بانتظام، على الأقل كل ثلاثة إلى ستة أشهر. (هناك مثل قديم يقول أنه عليك تغيير كلمة المرور في كل مرة تقوم بتغيير فرشاة الأسنان: وهذا يجب أن يحصل كل ثلاثة إلى أربعة أشهر كما ينصح تسعون بالمائة من أطباء الأسنان).

عندما تغير كلمة المرور، حاول أن تبتكر كلمة مرور جديدة لم تقم باستخدامها من قبل. يخطئ الكثير من الأشخاص بإعادة استخدامهم نفس كلمات المرور مرات متتالية عندما يحين الوقت لتغييرها، ومن الجلي أن هذا خطر أمني كبير.

قوائم تحتوي جميع كلمات المرور

الحياة العصرية ليست سهلة، حيث يتوجب عليك أن تتذكر كلمات المرور الخاصة بتسجيل الدخول، كلمات المرور الخاصة بالبريد الإلكتروني، كلمات المرور الخاصة بمواقع الويب، أرقام التعريف الشخصية الخاصة بآلة الصرافة المؤتمتة ATM، بالإضافة إلى أعياد الميلاد والذكريات السنوية (وهي على الأرجح المعلومات الأكثر أهمية). لذلك لا داعي للعجب من استخدام معظم الأشخاص سلسلة من كلمات المرور السهلة والمنتشرة.

الحل الأبسط لهذه المشكلة هو الاحتفاظ بقائمة مشفرة من جميع كلمات المرور، يمكن أن تكون القائمة عبارة عن ملف نصي يحتوي جميع كلمات المرور التي تستخدمها ولماذا تستخدم، وهذا الملف مشفر باستخدام خوارزمية تشفير قوية مثل AES، BlowFish، وIDEA، إذا نسيت كلمة مرور ما عليك سوى فك تشفير القائمة واستخراج كلمة المرور. عندما تقوم بتغيير كلمة مرور ما، قم بفك تشفير الملف، قم بإجراء التغييرات، ومن ثم أعد تشفير الملف مرة أخرى. يمكنك بسهولة تخزين الملف على قرص مرن، المساعد الرقمي الشخصي، أو القرص الصلب. وإذا كنت مرتاباً قليلاً، يمكنك تخزين القائمة في ملف آخر باستخدام أحد برامج Steganography* التي مرت معنا في قسم "الإجراءات المضادة" من الفصل الخامس.

* تذكرة: Steganography هو علم وفن لإخفاء الرسائل السرية عن طريق تحويلها إلى شكل آخر يكون عادة ظاهراً بحيث يراه الجميع.

وتذكر أيضاً ما أخبرتك به جدتك بشأن وضع كل البيض في سلة واحدة. وبالتأكيد فإنك لا ترغب بأن يحصل الجاسوس على هذه المعلومات، لذلك اتبع الإجراءات التالية:

- ضمان أن تطبيق التشفير الذي تستخدمه موثوق وآمن.
- استخدام كلمة مرور قوية.
- ضمان عدم وجود أية طريقة ممكنة ليسرّب التطبيق أو نظام التشغيل نصاً غير مشفراً من الملف المشفر.

أحد طرق التحقق من وجود التسرّب هو استخدام محرر ست عشري، بعد تشفير الملف، وذلك عن طريق البحث ضمن كامل القرص الصلب عن نص فريد موجود فقط ضمن الملف المحمي، مثلاً أحد كلمات المرور. وفي حال وجدت النص، فإنه لدينا احتمالين، الأول قيان التطبيق بتسريب المعلومات وذلك عن طريق كتابة المعلومات إلى ملف مؤقت لا تعلم بوجوده، والثاني قيام نظام التشغيل بتسريب البيانات وذلك عن طريق حفظ المعلومات إلى ملف الترحيل Swap File. فإذا حصل هذا يجب عليك إنشاء قرص إقلاع لنظام التشغيل DOS يتضمن محرر نصوص بسيط وإصدار سطر الأوامر لبرنامج التشفير الذي تستخدمه، ثم أقلع الحاسب باستخدام هذا القرص وحافظ على قائمة كلمات المرور ضمنه.

يوجد خيار آخر، وهو استخدام تطبيق تجاري أو مجاني لإدارة كلمات المرور، تخزن هذه البرامج قاعدة بيانات مشفرة لكلمات المرور والمعلومات الهامة الأخرى. (يمكنك الحصول على مثل هذه البرامج مجاناً لنظام التشغيل Windows على الرابط www.webattack.com/Freeware/security/fwpass.shtml). بالرغم من أن برامج إدارة كلمات المرور ملائمة وسهلة الاستخدام، إلا أنه عليك أن تثق بمبرمج مجهول ومهاراته في تطوير منتج آمن.

بدائل لكلمات المرور

كلمة المرور هي ببساطة طريقة مصادقة، أسلوب للتمييز بين مستخدم وآخر، وبما أن كلمات المرور الضعيفة والنصية معرضة للمهاجمات الدائمة ومن الصعب إقناع الناس باستخدام كلمات مرور قوية، وجدت أساليب مصادقة أخرى تؤمن حماية أفضل. سوف نغطي بعضاً من أنواع أجهزة المصادقة التي يمكن أن تستخدمها حالياً أو في المستقبل القريب.

الأجهزة الحيوية Biometrics

تعتمد الكثير من أجهزة المصادقة البديلة على أساليب حيوية. حيث تعتمد الأجهزة الحيوية، بدلاً من استخدام نظام نموذجي لكلمات المرور يعتمد على ما تعرفه (أي كلمة المرور)، على بعض المواصفات الفيزيائية الفريدة التي تملكها، أي بشكل أساسي ما أنت عليه.

حالياً، يتم الترويج للأجهزة الحيوية عن طريق وسائل الإعلان والتسويق، بشكل أساسي بصفتها تقنية أمنية لكشف المجرمين المعروفين أو المشتبه بهم. أما فيما يتعلق بانتشار استخدام هذه الأجهزة، فهي لا تزال في بداية الطريق، لكن هناك بعض المشاكل التي تنتظر الحل قبل إمكانية استخدام هذه الأنظمة بشكل فعال. من المهم أن تتعرف على مصطلحين يتعلقان بدقة الأنظمة الحيوية:

- درجة الرفض الزائف False Rejection Rate (FRR) عندما لا يصادق الجهاز بشكل صحيح مستخدماً مخولاً.
- درجة القبول الزائف False Acceptance Rate (FRR) عندما يصادق الجهاز عن طريق الخطأ مستخدماً غير مخولاً.

من الهام معرفة قيم FRR وFAR، وخاصة إذا حصلت على الأرقام من فحوصات المختبر أو من الاستخدام الفعلي الأكثر تعقيداً وصرامة. كما عليك أيضاً أن تفهم بعض نقاط الضعف المحتملة إذا كنت ترغب باقتناء نظاماً حيوياً، وبما فيها ما يلي:

- **مهاجمات الإعادة:** يقوم المكوّن الصلب للنظام الحيوي بتمرير البيانات إلى المكوّن البرمجي للنظام لتتم مصادقة المستخدم. إذا تم التقاط البيانات التي تم التحقق منها يمكن أن يتم إعادتها مرة أخرى إلى المكوّن البرمجي للنظام لتحقيق الوصول. مثلاً، من الممكن التقاط تسلسل مصادقة ناجح، باستخدام ماسح البصمات المتصل بمدخل USB، ومن ثم إعادة هذا التسلسل عبر المدخل في وقت لاحق.
- **الانتحال:** بما أن الأجهزة الحيوية تعمل عن طريق التعرف على صفة فيزيائية لشخص ما، فمن الممكن خداع الجهاز باستخدام نسخة لتلك الصفة. فعلى سبيل المثال، يمكن انتحال نظام التعرّف على الصوت عن طريق مسجل رقمي وذلك لتسجيل نسخة من كلمات المستخدم.
- **التلاعب بقاعدة البيانات:** تحتاج التواقيع الحيوية إلى أن تخزن في قاعدة بيانات لإجراء المقارنة أثناء عملية المصادقة، ومن الممكن أن يتلاعب الجاسوس بقاعدة البيانات وأن يضيف دخولاً بشكل سري لمنح شخص غير مخول الإذن بالدخول إلى النظام.
- **مبدأ الهندسة العكسية:** تتألف جميع الأجهزة الحيوية من المكوّنات الصلبة وبعض البرمجيات التي تتصل بنظام التشغيل أو بالتطبيق. من الممكن إجراء هندسة عكسية للبرمجيات بحيث تقوم خوارزمية التعرّف دوماً بالمصادقة على هوية المستخدم حتى لو لم يظهر في قاعدة بيانات النظام. لقد تحايل المخرّبون لسنوات طويلة وحتى الآن على خطط حماية النسخ، وذلك ببساطة عن طريق تغيير قيمة ست عشرية لعبارة تفريع شرطية مكتوبة بلغة assembly أو استبدال شيفرة برمجية بتعليمة عملية معدومة. إذا كان مخرّب مراهق يستطيع

أن يقوم بإجراء الهندسة العكسية والتغلب على مخطط معقد لحماية البرمجيات، فمن الممكن جداً أن يتم اختراق برنامج نظام المصادقة.

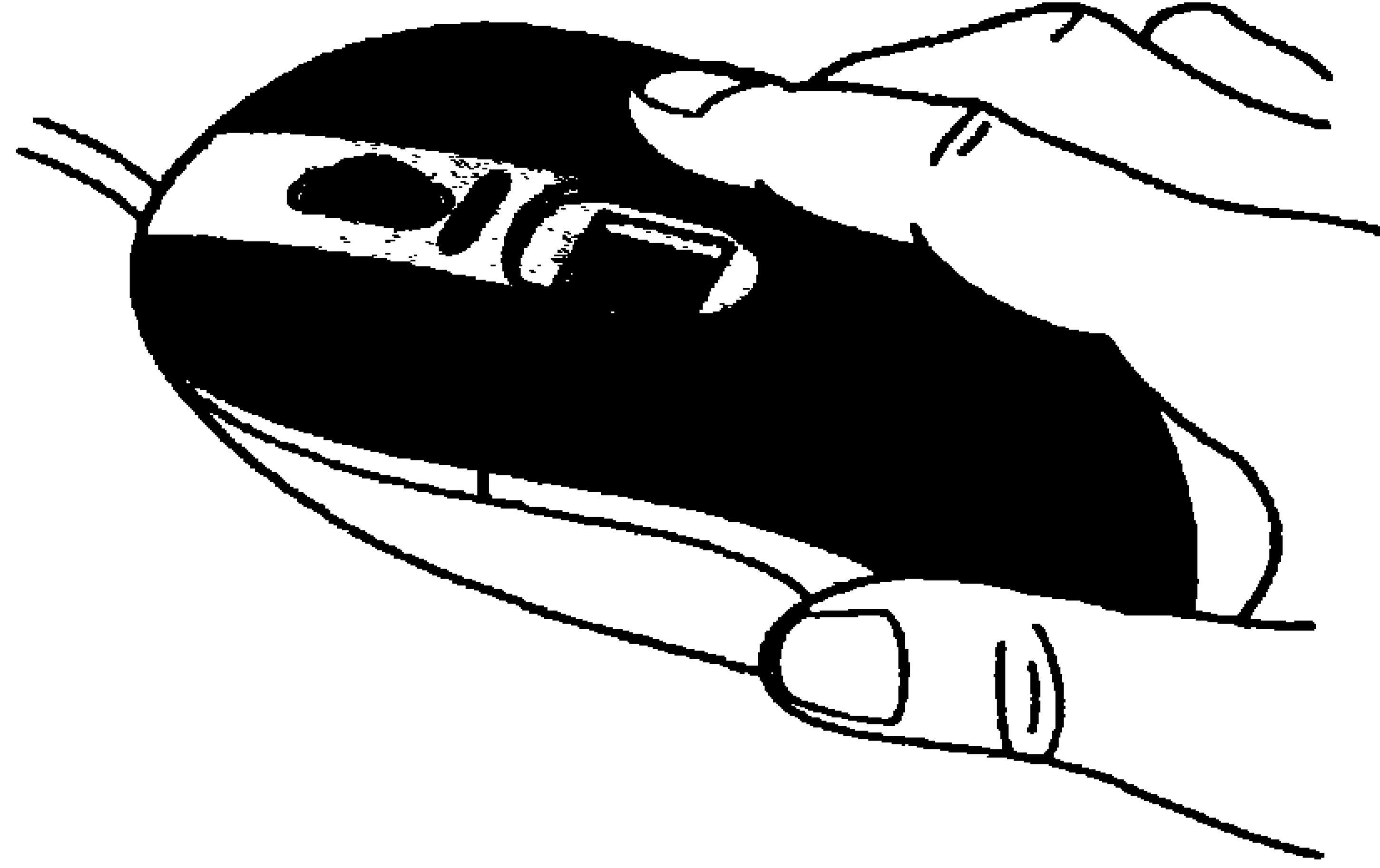
وبما أن الأجهزة الحيوية أصبحت شائعة ومستخدمة بصورة أوسع، سوف يتم اكتشاف ونشر نقاط ضعف جديدة. يجب ألا تعتمد الأجهزة الحيوية، مثل التقنيات الأخرى، على حماية المعلومات الحساسة فقط، إنما يجب أن تكون جزءاً من نظام أمني متكامل.



أبرزت مجلة ألمانية للحواسب مقالة في إصدارها في شهر تشرين الثاني من عام 2002، حيث حاول مجموعة من المختبرين أن يجربوا أحد عشر جهازاً حيوياً. وانتهوا بالتغلب على هذه الأجهزة بعد مجموعة من المهاجمات البسيطة. تتوفر الترجمة باللغة الإنكليزية لهذه المقالة على الرابط http://heise.de/ct/english/02/11/114/.

ماسحات بصمات الأصابع FINGERPRINT SCANNERS: وهي أجهزة المصادقة الحيوية الأكثر استخداماً حالياً. تتراوح تكلفة النماذج المصممة للمستهلك بين 100 و150 دولار أمريكي، وتعمل عن طريق التعرف على نماذج أطراف الأصابع باستخدام ماسحات أصابع صلبة خارجية مع وجود بعض الأنواع التي تكون مدمجة في لوحات المفاتيح والفأرة، كما هو موضح في الشكل 3-6. يتم في البداية فحص البصمة المخولة وتخزن في قاعدة بيانات (لا يتم تخزين صورة رقمية للبصمة، مثل التي تأخذها الشرطة: وبدلاً من ذلك تسجل كسلسلة من النقاط وتخزن في ملف يحوي تفصيلات دقيقة وكاملة ذو حجم 256 بايت). يفحص نظام المصادقة بصمات الأصابع المتلاحقة ويتحقق من وجود تطابق مع إحداها. إذا كانت بصمتك موجودة في قاعدة البيانات بإمكانك عندئذ الوصول إلى النظام، أما إذا لم تكن كذلك، فلن تتمكن من الدخول إلى النظام.

تعاني أنظمة التعرّف على بصمات الأصابع من مجموعة من السيئات، فهي تتأثر بالدثور العادية على أطراف الإصبع، الندبات، العرق، والأقذار. بالإضافة إلى ذلك إذا تمكن خصمك من الوصول إلى إصبعك (سواء متصلاً بك أو مقطعاً) أو نسخة قريبة جداً منه، فهناك احتمال لا بأس به أن يتم اختراق الأمن لديك.



الشكل (6-3) جهاز مصادقة عن طريق مسح بصمات الأصابع مركب داخلياً في الفأرة.

أساليب: التعطل عن العمل

ألقى الباحث Tsutomu Matsumoto من الجامعة الوطنية في ولاية Yokohama محاضرة حول مساوئ ماسح بصمات الأصابع، في شهر أيار عام 2002، وأصدر مقالة في نفس الوقت.

حيث صنع إصبعاً هلامياً مزوراً، باستخدام تجهيزات منزلية شائعة كلفتها أقل من عشرة دولارات، اخترق عدداً من ماسحات بصمات الأصابع التجارية المتوفرة.

صنع Matsumoto قوالب بلاستيكية لأصابع بعض الأشخاص المتطوعين ومن ثم ملأ القوالب بالهلام. وقد تمكنت البصمات المأخوذة من القالب بتجاوز ماسحات البصمات بنسبة ثمانين بالمائة. كما حاول Matsumoto أيضاً بنزع البصمات المنتشرة على الزجاج وقد نجح بشكل مماثل في صنع أصابع مزيفة مبنية على البصمات التي تخترق الماسح.

لقد نفى مصنّعو ماسحات البصمات سريعاً عمل Matsumoto، قائلين بأن عمله كان منجزاً تحت ظروف المختبر. ومع ذلك قدر معظم خبراء الأمن هذا العمل واعتبروه سبباً قوياً لعدم الاعتماد على ماسح البصمات كأسلوب وحيد لتأمين البيانات العالية الدقة.

يمكنك الإطلاع على محاضرة Matsumoto، والتي تتضمن صوراً ملونة وتعليمات لصنع الأصابع الاصطناعية من خلال الرابط:

www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf.

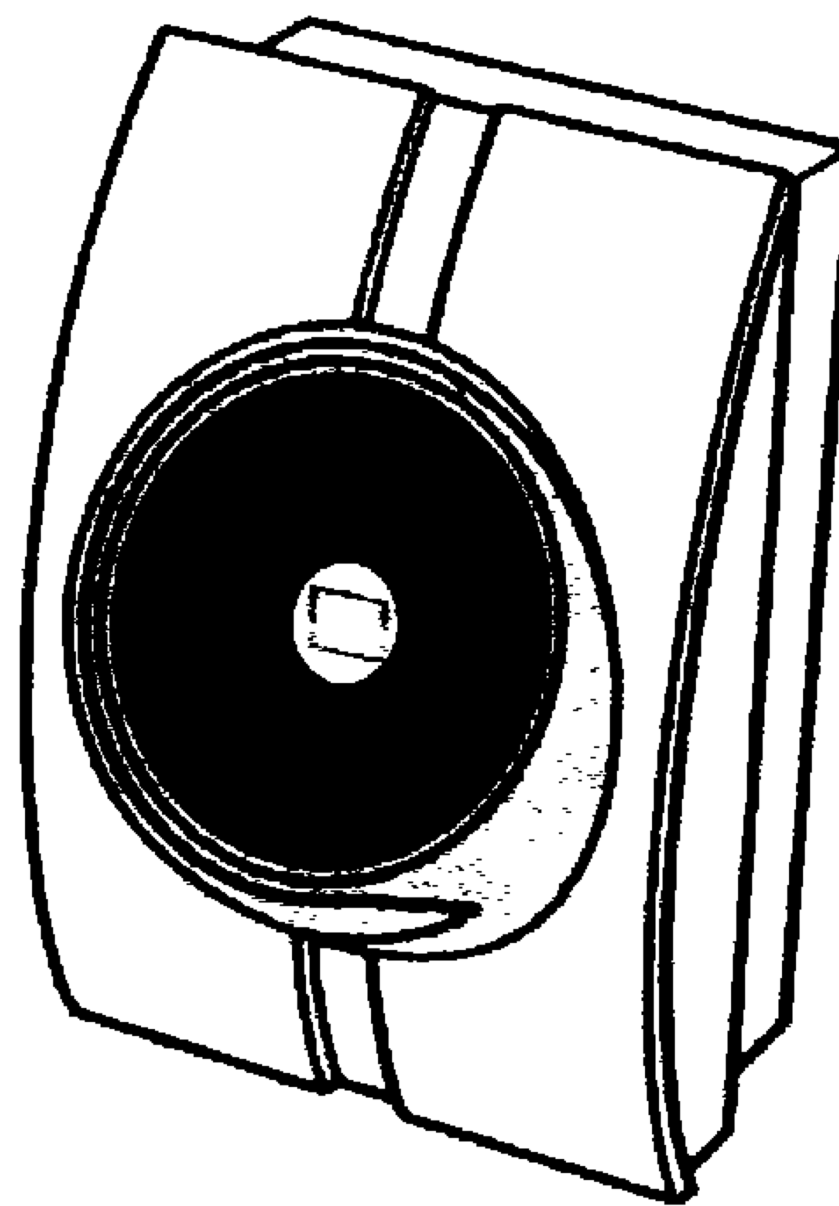
ماسحات العين البشرية EYE SCANNERS: يمكن تصنيف أجهزة المصادقة من خلال مسح العين البشرية إلى نوعين مختلفين. الأول ماسح لشبكية العين والتي تتراوح كلفته بين 400 إلى

500 دولار أمريكي، ويعمل بتسليط ضوء من الأشعة تحت الحمراء ذات الكثافة المنخفضة من خلال بؤبؤ العين إلى الأوعية الدموية ومن ثم إلى مؤخرة العين. هذه الأجهزة دقيقة للغاية وتوجد غالباً في المنظمات ذات الأمن الحرج. والثاني ماسح لقزحية العين، انظر الشكل 6-4، ويعتمد على تقنية امتلاكية وتتراوح تكلفته ما بين 200 و 300 دولار أمريكي. وهو أقل اختراقاً للعين من ماسح الشبكية لأنه يسجل سلبياً طراز النقاط والميزات الأخرى التي تظهر ضمن القزحية. بالمقارنة مع ماسحات الشبكية التي تم إثبات فعاليتها وأمنها، تم اختراق ماسحات القزحية باستخدام صور مفصلة للعين البشرية.

ماسحات الصوت VOICE SCANNERS تلتقط أجهزة فحص الأصوات مواصفات صوت الإنسان، مثل النغمة والنبرة وتردد الصوت. وبما أنه تتضمن معظم الحواسب محولات للصوت مع مداخل للميكرفون، فمن الممكن استخدام هذه التقنية بسهولة وفعالية ودون أي تكاليف إضافية. تتأثر دقة على الأجهزة الحيوية الصوتية بالبيئات الصاخبة، الميكروفون منخفض الجودة، والأمراض التي قد تؤثر صوت الإنسان مثل الزكام. تبلغ تكلفة هذه الأجهزة ما بين 150 إلى 200 دولار أمريكي.



يمكنك الحصول على مزيد من المعلومات حول أنظمة المصادقة الحيوية من خلال اتحاد الأجهزة الحيوية على الرابط (www.biometrics.org)، أو من خلال البحث الحيوي لجامعة ولاية Michigan على الرابط:
(http://biometrics.cse.msu.edu).



الشكل (6-4) جهاز مصادقة لمسح قزحية العين يقوم بتسجيل الطرازات في القزحية والميزات عندما تنظر في العدسة. لا تسلط ماسحات القزحية شعاعاً ضوئياً إلى العين على خلاف ماسحات الشبكية.

البطاقات الذكية SMART CARDS

البطاقة الذكية هي عبارة عن بطاقة بلاستيكية حجمها يعادل حجم بطاقة الاعتماد وتتضمن معالجاً صغرياً مثبتاً في داخلها، ويطلق على هذه البطاقات الصفة "ذكية" لأنها تملك معالجاً، ذاكرة، ونظام تشغيل خاص بها. تعمل هذه البطاقات على مبدأي مصادقة، وذلك لأسباب أمنية، شيء تملكه وشيء آخر تعرفه. عندما يتم إدخال البطاقة إلى قارئ بطاقات خارجي (يتم حالياً إدخال معظم البطاقات مباشرة إلى مداخل USB كلية، مقلصة الحاجة إلى قارئ)، تعرّف البطاقة نفسها إلى البرنامج كجزء من عملية المصادقة: ومن ثم يتوجب على المستخدم أن يدخل رقم التعريف الشخصي PIN الصحيح، ليتمكن من الوصول إلى الحاسب أو الشبكة.

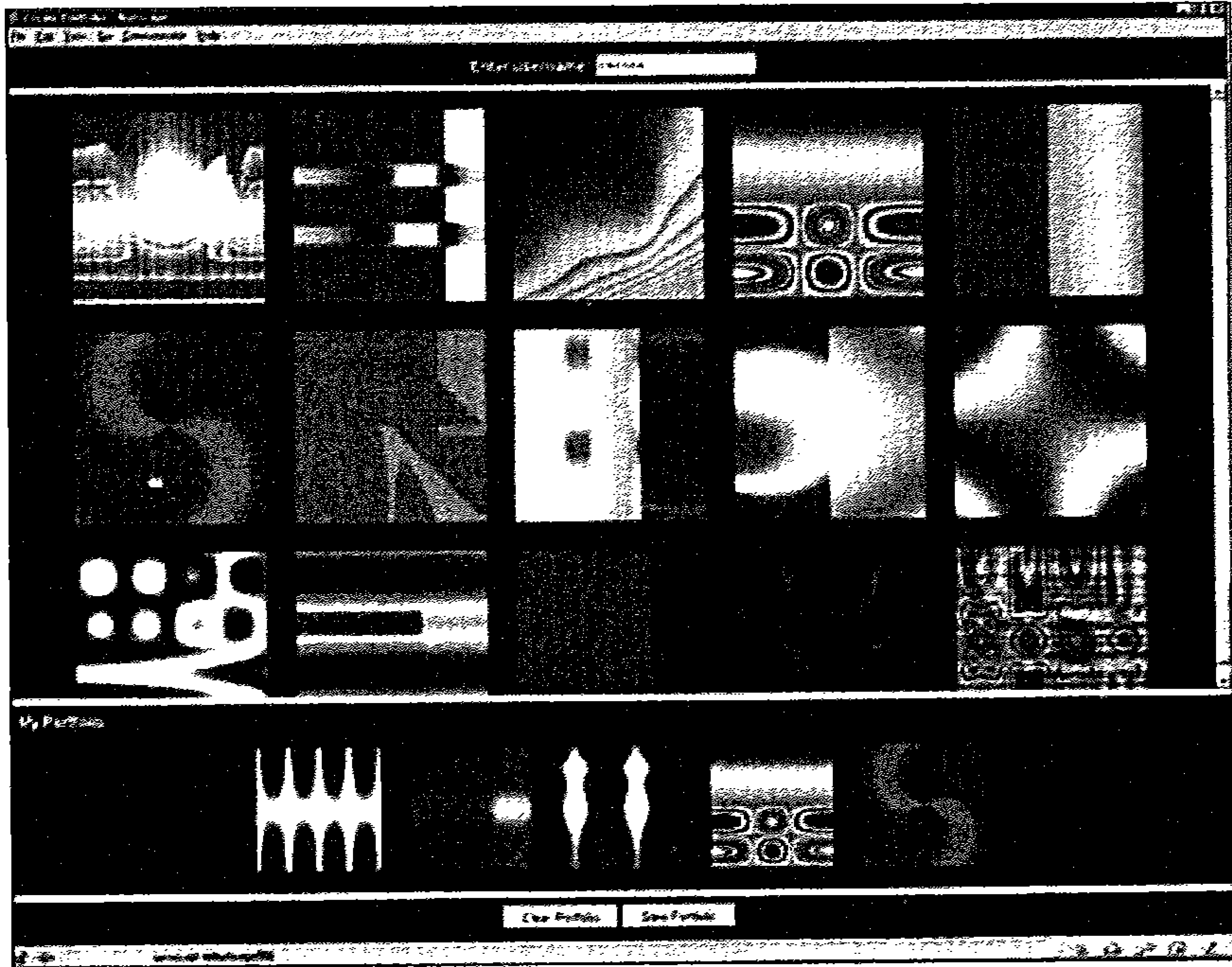
بالرغم من أن البطاقات الذكية هي طريقة آمنة للمصادقة، إلا أنه توجد مهاجمات يمكن أن يطبقها خصم ماهر تقنياً. يوجد موقع شامل مخصص لأمن البطاقات الذكية يمكنك زيارة الموقع من خلال الرابط www.geocities.com/ResearchTriangle/Lab/1578/smart.htm.

التعرف على الرموز SYMBOL RECOGNITION

هناك طريقة مصادقة غير حيوية أخيرة مبنية على التعرف على رمز، صورة، أو نموذج. حيث بدلاً من كتابة كلمة مرور نصية، تظهر سلسلة من الصور بشكل عشوائي ضمن نافذة، حيث يختار المستخدم الصور الصحيحة أو سلسلة من الصور باستخدام الفأرة والمؤشر لتتم عملية المصادقة. لقد أظهرت الدراسات أن تذكر الرموز أسهل من تذكر كلمات المرور النصية، ومن الجلي أنها أقل عرضة لمهاجمات القاموس (وقد تم إجراء بحث لتحديد فيما إذا كانت الصور الجميلة تبعث السرور لمعظم الأشخاص ولذلك تعتبر ضعيفة). طور المبرمجان Rachna Dhamija و Adrian Perrig نظاماً تجريبياً يدعى Déjà Vu، انظر الشكل 5-6، الذي يوضح مفهوم المصادقة هذا، ولمزيد من المعلومات اتبع الرابط www.sims.berkeley.edu/~rachna/dejavu.

ملخص

قد لا تكون المعلومات والأدلة التي قمت بحمايتها ظاهرياً آمنة بالشكل المطلوب. يشكل التشفير السيئ وكلمات المرور الضعيفة منفذاً سهلاً للجاسوس ليكشف البيانات المحمية مستخدماً أدوات كثيرة متنوعة سهلة الاستخدام.



الشكل (6-5) نظام التعرف Déjà Vu، ويظهر الرسوميات التي يختارها المستخدم.

إذا كنت تملك مستندات بالغة الأهمية على حاسبك، فلا تعتمد على مخططات الحماية المتوفرة في البرمجيات التجارية لحماية بياناتك. وبدلاً من ذلك عليك استخدام تطبيقات التشفير القوي. كما عليك أن تدرك بشكل كامل المخاطر المرتبطة بكلمات المرور والالتزام بسياسة لكلمات المرور التي تقلص خطر المهاجمات التي تعتمد على كلمات المرور الضعيفة.



نسخ البيانات

عندما يتمكن الجاسوس من الوصول فيزيائياً إلى حاسب ما، فسوف يرغب بالتأكيد بنسخ المعلومات الهامة منه. قد تظن أن هذا أمر بسيط ولا يستحق فصلاً كاملاً، لكن في الحقيقة هناك عدد من الاعتبارات والخيارات فيما يتعلق بنسخ البيانات والتجسس الحاسي.

تملك وسائط التخزين مثل الأقراص المرنة، الأقراص المضغوطة، وأقراص ZIP محاسن ومساوئ خاصة بها عندما يتعلق الأمر بالتجسس. كما أنه عليك أن تأخذ فكرة عن عدد من الأجهزة الخارجية التي توصل إلى الحاسب الهدف والمصممة خصيصاً لنسخ البيانات. والكثير من هذه المنتجات رخيصة ومتوارية عن الأنظار.

على خلاف معظم فصول هذا الكتاب والتي تحوي فقرة "الإجراءات المضادة" بعد الفقرة "أساليب الجواسيس"، لا يتضمن هذا الفصل هذه الفقرة، وذلك لأنك إذا طبقت جميع طرق الدفاع التي استعرضناها في باقي الفصول مثل الأمن الفيزيائي، التشفير، وكلمات المرور القوية فإنك ستمنع أي جاسوس من الوصول إلى الحاسب الهدف ومن استعراض البيانات المخزنة ضمنه.

لننتقل الآن إلى عملية نسخ البيانات من وجهة نظر الجاسوس.

أساليب الجواسيس

قبل أن نستعرض وسائط التخزين وأدوات التقانة المتطورة، توجد أربعة إرشادات لنسخ البيانات والتي يجب أن تتذكرها دائماً قبل أن تواجه الحاسب الهدف:

- استخدام الموارد المتوفرة. عليك أن تستفيد من أجهزة التخزين الموجودة مسبقاً لنسخ البيانات.
- استخدام أدوات الضغط. تأكد من حيازتك لبرامج الضغط في حال لم تتسع البيانات على وسائط التخزين.

- البيانات الأخرى. ليس عليك التركيز فقط على الأقراص الصلبة باعتبارها المصدر الوحيد للبيانات.
- إدراك ماذا يستخدم في نسخ البيانات. عليك التدرّب على نسخ البيانات بشكل مسبق.

استخدام الموارد المتوفرة

يؤيد الاستراتيجي الصيني Sun Tzu دائماً استخدام موارد عدوك لمصلحتك الشخصية، وعليك تطبيق نفس المبدأ في عملية نسخ البيانات. حيث سيحوي الحاسب الهدف محركاً للأقراص المرنة على الأقل، وإذا حالفك الحظ سيحوي مسجل الأقراص المضغوطة ومحرك الأقراص ZIP. كما يمكن أن يحوي برنامج للنسخ الاحتياطي منصب على الحاسب.

ما لم تحتاج إلى صورة شرعية عن القرص الصلب، يمكنك استخدام هذه الموارد لمصلحتك أثناء نسخ الملفات. عليك دائماً إحضار مجموعة من الأقراص المرنة الفارغة، الأقراص المضغوطة القابلة للتسجيل CD-R، الأقراص المضغوطة القابلة لإعادة التسجيل CD-RW، وربما قرص ZIP و Jaz لتتمكن من مضاعفة البيانات في حال عدم توفر أي أجهزة يمكنك أن تستخدمها.

استخدام أدوات الضغط

بالإضافة إلى جلب وسائط التخزين الفارغة، يجب أن يتضمن القرص أو القرص المضغوط أحد أنواع أدوات الضغط (مثل Gzip، WinZip، أو WinRAR)، وذلك لتستخدمها في حال كانت البيانات المطلوبة كبيرة الحجم لتتسع على وسائط التخزين لديك. تذكر أن ضغط البيانات يزيد من وقت عملية النسخ، وفي بعض الأحيان كل ثانية تكون مهمة.



أدوات الضغط ليست متماثلة من حيث السرعة وفعالية الضغط يمكنك الاطلاع على مقالة كتبها Martin Tsachev والتي تتضمن مقارنة بين أدوات الضغط على الرابط martin.f2o.org/windows/archivers.

البيانات الأخرى

تذكر أن القرص الصلب ليس المكان الوحيد التوضع البيانات. يمكن أن تتضمن الأقراص المرنة، الأقراص المضغوطة، أو الأشرطة الاحتياطية الملقية على المكتب، المخبأة على المكتب، أو التي تمت أرشفتها ضمن خزانة لحفظ الملفات معلومات مفيدة وقيمة، ويجب أن يتم نسخها أو

سرقتها إذا لم تعتقد أنه سيتم تفويتها. إذا اعتمدت على التسميات واعتقدت أن وسائط التخزين تتضمن محتويات احتياطية للقرص الصلب، قم بفحص الحاسب الهدف لمعرفة نوع أدوات الضغط المستخدمة لتعرف ما هو نـــوع التطبيـــق الذي ســـوف تستخدمـــه فيما بعد لتسترجع البيانات.

إدراك ماذا يستخدم في نسخ البيانات

كلما زادت مدة نسخك للبيانات، زادت احتمالات فشلك وفضح أمر وجودك، حيث يجب أن تدرك إمكانيات وقيود تقنيات النسخ المختلفة ووسائط التخزين.

من المهم جداً اعتبار معدل نقل البيانات Transfer Rate، وهو عبارة عن كمية البيانات الأعظمية التي يمكن نقلها نظرياً إلى الجهاز في غضون ثانية واحدة، ويتم استخدام الوحدات MBps (megabytes per second)، Mbps (megabits per second)، و Kbps (Kilobytes per second) (سوف نستخدم هذه الاختصارات الثلاثة خلال بقية الفصل عند وصف وسائط التخزين المختلفة). سوف تملك وقتاً محدوداً أمام الحاسب، وتشير وسائط التخزين التي تقوم باستخدامها إلى مدة نسخ كمية معينة من البيانات. (هناك أمور أخرى تؤثر على الفترة الزمنية اللازمة لمضاعفة البيانات مثل سرعة نقل الممر ونوع الوسائط التي تتوضع ضمنها البيانات، لكنك لا تستطيع التحكم بهذه العوامل).

عليك التدرّب على نسخ البيانات بشكل مسبق باستخدام أدوات نسخ مختلفة وأجهزة تخزين متنوعة لتتكون لديك فكرة مسبقة عن كمية الوقت والجهد اللازمين لمضاعفة البيانات.

خطر: تكنولوجيا منخفضة، مجازفة كبيرة

اقتحم أحدهم، في الرابع عشر من كانون الأول عام 2002، مكاتب شركة اتحاد العناية بالصحة TriWest في منطقة Phoenix في ولاية Arizona. ولم يكن هذا الاقتحام بهدف السرقة التقليدية، حيث قام اللص بالوصول إلى مكتب المدير الخاص، سرق المفتاح الرئيسي الخاص بالمدير، ومن ثم اقتحم تسهيلات الشركة. لم تتواجد كاميرات مراقبة لتصوير عملية الاقتحام، لكن أظهرت تسجيلات الدخول للباب الإلكتروني أن اللص أو اللصوص قد قاموا بعمليتي دخول وخروج من مكتب الشركة الكائن في الحديقة الصناعية في شمال غرب منطقة Phoenix.

أياً كان المقتحم فإنه كان يعرف ماذا يفعل، حيث قام بسرقة الأقراص الصلبة من الملقمات المستخدمة لتخزين تسجيل التأمين ومعلومات حول الادعاءات. كما تضمنت السجلات بيانات



شخصية لأكثر من 550,000 مستفيد من شبكة العناية المنظمة من قبل شرطة الولايات المتحدة، عبر 16 ولاية. (لا توجد معلومات فيما إذا كانت البيانات المسروقة مشفرة أم لا).

يحقق مكتب التحقيقات الفدرالي وخدمة التحقيقات الجنائية حول حادثة السرقة، ووعدت الشركة بتقديم جائزة بقيمة 100,000 دولار أمريكي مقابل الحصول على معلومات تقود إلى الاعتقالات وإرسال رسائل إلكترونية إلى المستفيدين المتضررين لتحذيرهم عن احتمال سرقة الهوية الشخصية، كما تراجع وزارة الدفاع إجراءات أمن تخزين البيانات للمتعاقدين المدنيين. حتى الآن لا يوجد مشتبه بهم، كما أن دافعهم غير معروف، ولا أحد يتكلم عن إجراءات التحقيق (ويمكن اعتبار وجود احتمال تورط الأمن الوطني والجنائي).

تظهر السرقة بوضوح مدى إمكانية كون البيانات العالية الدقة والهامة قديمة الطراز ومعرّضة لمهاجمات ليست ذات مستوى عالي، حتى في حال عدم ارتباطها بالتجسس. حيث أن المهاجمة الأكثر خفية كانت سوف تتم بطريقة أخرى، حيث من الممكن أن يتم استبدال الأقراص الصلبة المسروقة بمحركات متضررة أو غير مهيأة من نفس النوع. ومن ثم كان مدير النظام سيتمكن من القضاء على الأقراص باستخدام جهاز مناسب واستبدالها بأقراص أخرى ومن ثم استرجاع البيانات من النسخ الاحتياطية، حيث إذا تمت العملية بصورة صحيحة لم تكن الشركة قد شكت بموضوع سرقة بياناتها.

وسائط التخزين إلى الهدف

لننتقل الآن بعد الإرشادات السابقة لمناقشة وسائط التخزين المحمولة والشائعة الاستخدام والتي تستطيع باستخدامها نسخ البيانات (وسائط التخزين الكبيرة، الحديثة، والغريبة هي خارج نطاق هذا الكتاب).

الأقراص المرنة Floppy Disks

يفترض الجواسيس أن بإمكانهم أن يضعوا بسهولة قرصاً مرناً صغيراً 3.5 بوصة مليئاً بالأسرار في جيب قميصهم ومن ثم يخرجون من المبنى شكل عرضي دون أن يلتقطوا. لكن هذا لا يحدث في جميع الأوقات.

قدمت شركة IBM في عام1971 ما يسمى "قرص الذاكرة Memory Disk": وهو القرص المرن الأول (سمي بالمرن لأنه كان مرناً وليس صلباً) كان حجمه ثمانية بوصات، قابل للقراءة فقط، وسعته التخزينية 100KB فقط. لقد أحدث هذا المنتج ثورة كبيرة لأنه كان صغيراً ومحمولاً، حيث لم تكن تحتاج أن تجر البطاقات أو الأشرطة المغناطيسية من أجل نقل البيانات بين

الحواسب. وبعد عدة سنوات أطلقت شركة IBM إصداراً آخر لقرص قابل للقراءة والكتابة، سعة تخزينه وصلت إلى 250KB. التقنية الأساسية في محركات الأقراص هذه لا تزال موجودة في محركات الأقراص المرنة العصرية.

من تلك اللحظة، أصبحت الأقراص المرنة أصغر حجماً وأكبر سعةً. ظهر القرص5.25 بوصة عام 1976، وبلغت سعة تخزينه 100KB فقط. لكن سرعان ما اكتشف الباحثون كيفية الكتابة على كلا جانبي القرص وزيادة كثافته، وبلغت سعته بعد ذلك 1.2MB.

وأخيراً في عام 1981 أصدرت شركة Sony قرصاً مرناً ومحركاً للأقراص المرنة 3.5 بوصة، والذي استبدل في نهاية الأمر محرك الأقراص 5.25 بوصة واعتبر معياراً صناعياً. مواصفات هذا القرص أنه صغير الحجم، مغلف بغلاف بلاستيكي قاسي، ثنائي الجوانب، ذو كثافة مزدوجة، سعة تخزينه 1.44MB من البيانات، ومعدل نقل البيانات يبلغ 500Kbps، تكلفة كل قرص أقل من عشرين سنتاً.

يعتقد معظم الناس حالياً أن الأقراص المرنة قد انقرضت بسبب سعة تخزينها الصغيرة، هذا الأمر صحيح فيما يتعلق بنسخ كميات كبيرة من البيانات أو الملفات الكبيرة، لكن في نفس الوقت القرص المرن مفيد جداً فيما يتعلق بنسخ كميات صغيرة من البيانات واستخدامها في نشاطات تجسسية أخرى. استخدم كل من Robert Hanssen، Aldrich Ames، وAna Belen Montes المدانين الأقراص المرنة أثناء عمليات التجسس التي قاموا بها ضد حكومة الولايات المتحدة وذلك من أجل تلقي التعليمات من رؤسائهم وبهدف تمرير المعلومات المسروقة في المواقع المختارة (موقع محدد مسبقاً حيث تترك المعلومات أو التجهيزات بصورة سرية للجاسوس من قبل رئيسه، أو بالعكس، دون أن يحصل بينهما أي اتصال فيزيائي).

الأقراص المضغوطة القابلة للتسجيل CD-R، الأقراص المضغوطة القابلة لإعادة التسجيل CD-RW (CD-R/CD-RW)

لقد استبدل القرص المضغوط CD (Compact Disk) القرص المرن الكلي الوجود لكثير من مستخدمي الحاسب بصفته وسط التخزين الملائم. ولقد انتشرت محركات الأقراص المضغوطة القابلة لإعادة التسجيل CD-RW (والاسم الشائع لها ناسخات burners) كثيراً وأصبحت ميزة قياسية في الحواسب الجديدة، ومزودة بشعبية تحميل الموسيقى من شبكات الند للند P2P (peer to peer networks). وفيما يلي بعض مواصفات وسط التخزين هذا:

- يخزن قرص مضغوط وحيد، ذو حجم قياسي ما بين 650MB و 870MB من البيانات. تسمح الأقراص المضغوطة القابلة للتسجيل CD-R بكتابة البيانات عليها لمرة واحدة فقط، بينما الأقراص المضغوطة القابلة لإعادة التسجيل CD-RW تسمح أن تكتب البيانات وتحذف عدة مرات.
- الأقراص المضغوطة القابلة للتسجيل CD-R والأقراص المضغوطة القابلة لإعادة التسجيل CD-RW رخيصة، وتكلف بحسب كميتها أقل مما يتراوح بين خمسين سنتاً ودولاراً واحداً.
- يتم التعبير عن معدل النقل، والذي يعتمد على ناسخة الأقراص، بما يسمى سرعة الكتابة write speed. كلما زاد الرقم زادت سرعة الكتابة (كتابة البيانات إلى الأقراص المضغوطة القابلة للتسجيل CD-R أسرع من كتابة البيانات إلى الأقراص المضغوطة القابلة لإعادة التسجيل CD-RW). فعلى سبيل المثال، تستغرق ناسخة أقراص قديمة سرعة الكتابة لديها 8x (أي يصل معدل النقل إلى حوالي 1,200Kbps) عشر دقائق لمضاعفة قرص مضغوط، بينما يستغرق محرك الكتابة الشائع (ذو سرعة الكتابة 24x أي حوالي 3,600Kbps) أكثر بقليل من أربع دقائق لإنجاز نفس العمل. بدأت تظهر المحركات ذات سرعة الكتابة 52x في أواخر عام 2002، وهي ستحتل المركز الأعلى بالنسبة لسرعة الكتابة.

يأتي مع معظم ناسخات الأقراص برنامج يتعامل مع القرص المضغوط مثل القرص المرن بحيث يمكنك نسخ أو إنشاء الملفات مباشرة عليه (مثل، البرنامج الشائع DirectCD من شركة Roxio). إذا كنت تستخدم ناسخة من أجل نسخ البيانات إلى قرص مضغوط قابل للتسجيل CD-R على الحاسب الهدف، تأكد من أنك قد حددت خيار أن القرص المضغوط قابل للقراءة من قبل باقي الحواسب عند الانتهاء. حيث لا يسمح البرنامج الخاص بالقرص المضغوط الذي تتم معاملته كقرص مرن أن يتم الوصول إليه من حاسب آخر، كما في حالة القرص المضغوط القابل للقراءة فقط. فإذا كنت تستخدم برنامجاً للكتابة مباشرة، عليك قبل أن تزيل القرص المضغوط من المحرك أن تحدد أن القرص المضغوط قد تمت الكتابة عليه بحيث تتمكن باقي الحواسب من قراءته (بتنسيق ISSO 9660).

مضبوط: الأقراص الماكرة

تنص المستندات التابعة لمكتب التحقيقات الفدرالي أن الجاسوس المدان Robert Hanssen استخدم الأقراص المرنة بصورة متكررة لتمرير البيانات جيئة وذهاباً إلى رؤسائه في روسيا. وتوجد بعض المعلومات المشوقة والمثيرة في مذكرة اعتقاله تتعلق بالأقراص المرنة:

"تلقت وكالة الاستخبارات الروسية KGB في شهر نيسان (أبريل) عام 1988، مغلفاً من "B" من عنوان إقامة مؤقت في المقاطعة الشرقية من ولاية Virginia. كما حمل المغلف عنوان عودة باسم "Jim Baker" في الإسكندرية ومختوم بالختم البريدي في شمال Virginia، بتاريخ 31 من شهر آذار (مارس) عام 1988. تضمن المغلف نصاً من "B": 'استخدم نمط المسار 40. هذه الرسالة ليست إشارة' (use 40 TRACK MODE. This letter is not a signal)

يشير المصطلح "نمط المسار 40" إلى عملية تقنية لإعادة تهيئة قرص حاسبي بهدف إخفاء البيانات وذلك بوضعها ضمن مسارات محددة على القرص. وما لم يستخدم الشخص الشيفرة الصحيحة لفك تشفير هذا القرص، سوف يظهر القرص وكأنه فارغ."

إن الوصف الذي تزوده الشهادة الخطية السابقة حول عبارة "استخدم نمط المسار 40" غامض نوعاً ما وربما مضلل أيضاً باستخدامه الكلمة "فك التشفير". لم يتم نشر الكثير من التفاصيل الدقيقة لنشاطات التجسس التي قام بها Hanssen، وتوجد هناك عدة معاني قد تشير إليها العبارة النمط 40 لتوضح ما كان سيقوم به Hanssen.

- افتراضياً تتم تهيئة الأقراص المرنة 5.25 بوصة، ذات الحجم الثابت 320KB باستخدام أربعين مساراً. ومن الممكن أيضاً تهيئة قرص مرن 5.25 بوصة، الثنائي الجوانب 760KB و 1.2KB والذي يتضمن 80 مساراً ليحوي 40 مساراً فقط. هذا يؤدي إلى إخفاء البيانات على الجانب الآخر من القرص.
- أنشأ فيروس يصيب قطاع الإقلاع للقرص، يسمى Joshi، المسار 41، والذي قد يكون المسار 40، على قرص 5.25 بوصة، و 320KB وذلك لإخفاء الشيفرة داخله. قد يكون Hanssen قد قام بإخفاء البيانات في المسار الإضافي. (مع أنه تم اكتشاف الفيروس Joshi عام 1990، أي بعد سنتين من رسالة Hanssen الغامضة).
- استخدمت تقنية TRS-80 أقراصاً مرنة تحوي 35 مساراً، لكن وجد الهواة أن بإمكانهم أيضاً أن يهيئوا هذه الأقراص إلى 40 مساراً غير نظامياً. TRS تقنية قديمة بالنسبة لعام 1988، لكنها قد تكون مفيدة أحياناً في أعمال التجسس إذا افترض خصمك أنك تستخدم طريقة اتصالات عصرية.

ما يمكننا عمله الآن هو أن نفكر بدقة ما قد تعني عبارة المسار 40، حتى يتم نشر معلومات محددة أكثر للشعب حول حرفة Hanssen المرتبطة بالحواسب.

وسائل التجارة: الممر التسلسلي العالمي USB والمعيار IEEE 1394

لقد كان الممر التسلسلي العالمي USB والمعيار IEEE 1394 أحلام الجواسيس التي أصبحت حقيقة. عندما تستخدم هذه الأدوات مع نظام تشغيل يعمل على مبدأ ركّب ثم شغّل، كل ما

عليك فعله هو تركيب جهاز تخزين محمول مثل قرص صلب أو ناسخة أقراص مضغوطة إلى الحاسب وأن تبدأ بنسخ الملفات. قبل أن تسرع لشراء أحد هذه الأجهزة المحيطية الذكية، سنعرض بعض المعلومات عنها.

ظهر الممر التسلسلي العالمي لأول مرة عام 1997 بصفته طريقة جديدة للوصل بين الأجهزة المحيطية، لكنه لم ينتشر فعلياً إلا بعد أن أصدرت شركة Microsoft نظام التشغيل Windows 98 في شهر حزيران (يونيو) عام 1998. يدعم معيار الممر التسلسلي العالمي الأصلي USB 1.0/1.1 معدلاً بطيئاً نسبياً لنقل البيانات 12Mbps (megabits-per-second وليس MBps أي megabytes-per-second). ظهرت الحواسب ذات الإصدار USB 2.0 في صيف عام 2002، الإصدار الجديد للممر التسلسلي العالمي أسرع بكثير وينقل البيانات بسرعات تصل إلى 480Mbps. كما تظهر أجهزة تخزين أسرع في الأسواق حالياً والتي تستفيد من الإصدار USB 2.0 وهي متوافقة مع الإصدار الأقدم USB 1.1، وقد تواجه حالياً بعض الحواسب التي تدعم الإصدار الأقدم USB 1.1.

يشكل المعيار IEEE 1394 منافساً للممر التسلسلي العالمي USB (واسمه الشائع FireWire، وهو الاسم الشائع الذي أطلقته شركة Apple لهذا المعيار، أو الاسم التجاري i.Link الذي أطلقته عليه شركة Sony). ظهر المعيار IEEE 1394 منذ عام 1986، وتبناه المعهد IEEE (معهد المهندسين الإلكترونيين والكهربائيين Institute of Electrical and Electronic Engineers) كمعيار في عام 1995. لقد نشرت شركة Apple هذا المعيار كطريقة عالية السرعة لنقل البيانات الرقمية الصوتية والمرئية بين حواسب Macintosh والأجهزة الأخرى. وتصل سرعة أجهزة 1394 إلى 400Mbps. وتتم المنافسة بين منتجات المعيار 1394، التي بدأت بالظهور منذ بداية عام 2003، ضد معيار USB 2.0 بسرعات تصل إلى 800Mbps.

ومع أن شركة Microsoft قامت بدعم المعيار IEEE 1394 في نظام التشغيل Windows، إلا أنك على الأغلب ستصادف منافذ USB في معظم الحواسب التي قد تتجسس عليها. لمزيد من المعلومات حول أجهزة USB، بما فيها الأقراص الصلبة وناسخات الأقراص المضغوطة، اتبع الرابط www.everuthingusb.com.

الأقراص DVD (DVDs)

تشكل أقراص الفيديو الرقمي DVD (digital video discs أو digital versatile discs) الجيل القادم من وسائط التخزين الضوئي. يمكنك تشبيه قرص DVD بقرص مضغوط CD لكنه أسرع ويمكن أن يخزن 4.7GB من البيانات. مع انخفاض الأسعار (تصل تكلفة المحركات إلى أقل من 300 دولار أمريكي) وتبني المعايير، سوف تستبدل أقراص DVD الأقراص المضغوطة CD باعتبارها خياراً لوسط التخزين الحاسبي.

- تتصارع حالياً مجموعتان حول نوع الأقراص DVD التي ستصبح المعيار السائد، إما أقراص الفيديو الرقمي القابلة للتسجيل DVD-R، أقراص الفيديو الرقمي القابلة لإعادة الكتابة DVD-RW، أو أقراص الفيديو الرقمي القابلة للتسجيل وأقراص الفيديو الرقمي القابلة لإعادة الكتابة معاً DVD+R/DVD+RW. يحاول بعض المصنعين، مثل شركة Sony احتلال موقعاً غير متطرفاً وضمان أن محركات الأقراص DVD لديها تدعم كلا المعيارين.
- البيانات المكتوبة إلى قرص DVD بسرعة 1x مكافئة للسرعة 11Mbps، وهي تقريباً أسرع بتسع مرات من معدل نقل قرص مضغوط للقراءة فقط CD-ROM سرعته 1x. تستطيع المحركات الحالية الكتابة بسرعة تصل إلى 4x بالنسبة لأقراص الفيديو الرقمي القابلة للتسجيل DVD-R وبسرعة 2x بالنسبة لأقراص الفيديو الرقمي القابلة لإعادة الكتابة DVD-RW. (يمكنك باستخدام ناسخات أقراص DVD كتابة البيانات إلى الأقراص المضغوطة القابلة للتسجيل CD-R و الأقراص المضغوطة القابلة لإعادة التسجيل CD-RW).
- تتراوح أسعار أقراص الفيديو الرقمي القابلة للتسجيل DVD-R، بحسب النوعية، من 1.50 إلى 3.50 دولاراً أمريكياً للقطعة الواحدة، بينما أقراص الفيديو الرقمي القابلة لإعادة الكتابة DVD-RW مسعّرة بين 2.50 و4.50 دولار أمريكي. سوف تنخفض هذه الأسعار عندما تصبح هذه الوسائط منتشرة بشكل أوسع.

حالياً، من المحتمل أنك ستصادف حواسب ذات ناسخة أقراص مضغوطة أكثر من ناسخة أقراص DVD، لكن يجب أن تتزود ببعض أقراص DVD الفارغة للاحتياط.

أقراص ZIP (ZIP Disks)

قبل أن تصبح ناسخات الأقراص المضغوطة رخيصة وشائعة، جاءت محركات الأقراص ZIP من شركة Iomega (www.iomega.com) لتستبدل الأقراص المرنة باعتبارها المعيار الصناعي التالي لوسط التخزين القابل للإزالة. ظهرت محركات الأقراص ZIP عام 1994، وقدمت حجم 100MB من التخزين المؤقت، وشكل هذا القرص مثل القرص المرن المتنفخ. وقدمت لاحقاً نماذج محركات الأقراص ZIP حجم تخزين يصل إلى 750MB، وتخزن محركات Jaz ما يصل إلى 2GB من البيانات.

كانت الإصدارات الخارجية للمنفذ التفرعي لمحركات ZIP بطيئة جداً، مع معدل لنقل البيانات يتراوح بين 300 و 800Kbps، بينما تميزت الإصدارات الداخلية لإلكترونيات الأجهزة المتكاملة IDE (Integrated Device Electronics) بمعدلات نقل أسرع من 1.4MBps إلى 2.4MBps. مع

أن محركات Jaz ونماذج الأقراص ZIP المتلاحقة تميزت بمعدلات نقل أسرع، لكن استخدام هذه الأجهزة انحسر بسبب كلفة هذه الوسائط (من سبع إلى أكثر من عشر دولارات للقرص الواحد) وحلول ناسخات الأقراص المضغوطة والأقراص المضغوطة غير المكلفة. قد تصادف في بعض الأحيان محركات الأقراص ZIP متصلة بالحواسب القديمة نوعاً ما أو في بعض الميادين التخصصية (انتشرت هذه المحركات كثيراً بين الفنانين وأقسام الإبداع).

أجهزة التخزين في الذاكرة Memory Storage Devices

إذا لم تحتاج إلى نسخ كميات كبيرة من البيانات، فإن خيارك الأفضل هو استخدام أحد أنواع أجهزة التخزين ذات الذاكرة الومضية (flash memory storage device). هذه الأنواع من أجهزة التخزين خفية تماماً بسبب حجمها الصغير، كما أنها لا تحتاج إلى مصدر طاقة خارجي لأن الذاكرة الومضية هي ذاكرة دائمة (nonvolatile).

قم بتركيب بطاقة ذاكرة ومضية باستخدام محول إلى مقبس البطاقة في الحاسب المحمول (تحوي بعض الحواسب المحمولة مقابس تلائم مباشرة أنواعاً محددة من بطاقات الذاكرة) أو ركّب جهاز الذاكرة إلى قارئ البطاقات المتصل بالحاسب الشخصي المكتبي وابدأ بعملية النسخ.

لم تتفق صناعات الكاميرات الرقمية، الحواسب المحمولة، وأجهزة التسجيل الصوتية على نمط موحد للذاكرة الومضية، وبالتالي هناك عدد من الأنماط التي يمكن أن تختار منها:

- **CompaqFlash (CF)**: أول جهاز ذاكرة ومضية، مقدّم من قبل شركة SanDisk عام 1994 (وما يزال الأكثر انتشاراً).
- **MemoryStick**: جهاز الذاكرة الخاص بشركة Sony، ظهر في عام 1998.
- **Multimedia Memory Card (MMC)**: بطاقة ذاكرة صغيرة، حجمها مثل حجم الطابع البريدي تقريباً.
- **Secure Digital**: تتضمن بطاقة الذاكرة هذه مقبضاً للحماية من الكتابة بهدف الوقاية من مسح المحتويات عن طريق الخطأ.
- **SmartMedia**: أجهزة ذاكرة أصغر وأرفع من وحدات الذاكرة CF.

تناسب بطاقات الذاكرة من نوع CompaqFlash لأغراض التجسس، لأنها تتسع لبيانات أكثر بكثير من الأجهزة الأخرى وهي متينة جداً (أعلنت شركة SanDisk في آذار عام 2003، عن بطاقة ذاكرة حجمها 4GB والتي بدأت بالشحن في صيف ذلك العام، ومسعرة 999 دولاراً

أمريكياً). تدعم بطاقات CF Ultra الجديدة العالية السرعة معدلاً لنقل البيانات يصل إلى 2.8MBps، تقريباً ضعف سرعة بطاقات CF التقليدية. تتراوح تكلفة بطاقات الذاكرة 128KB بين 50 إلى 60 دولاراً أمريكياً حالياً (والأسعار مستمرة بالهبوط).



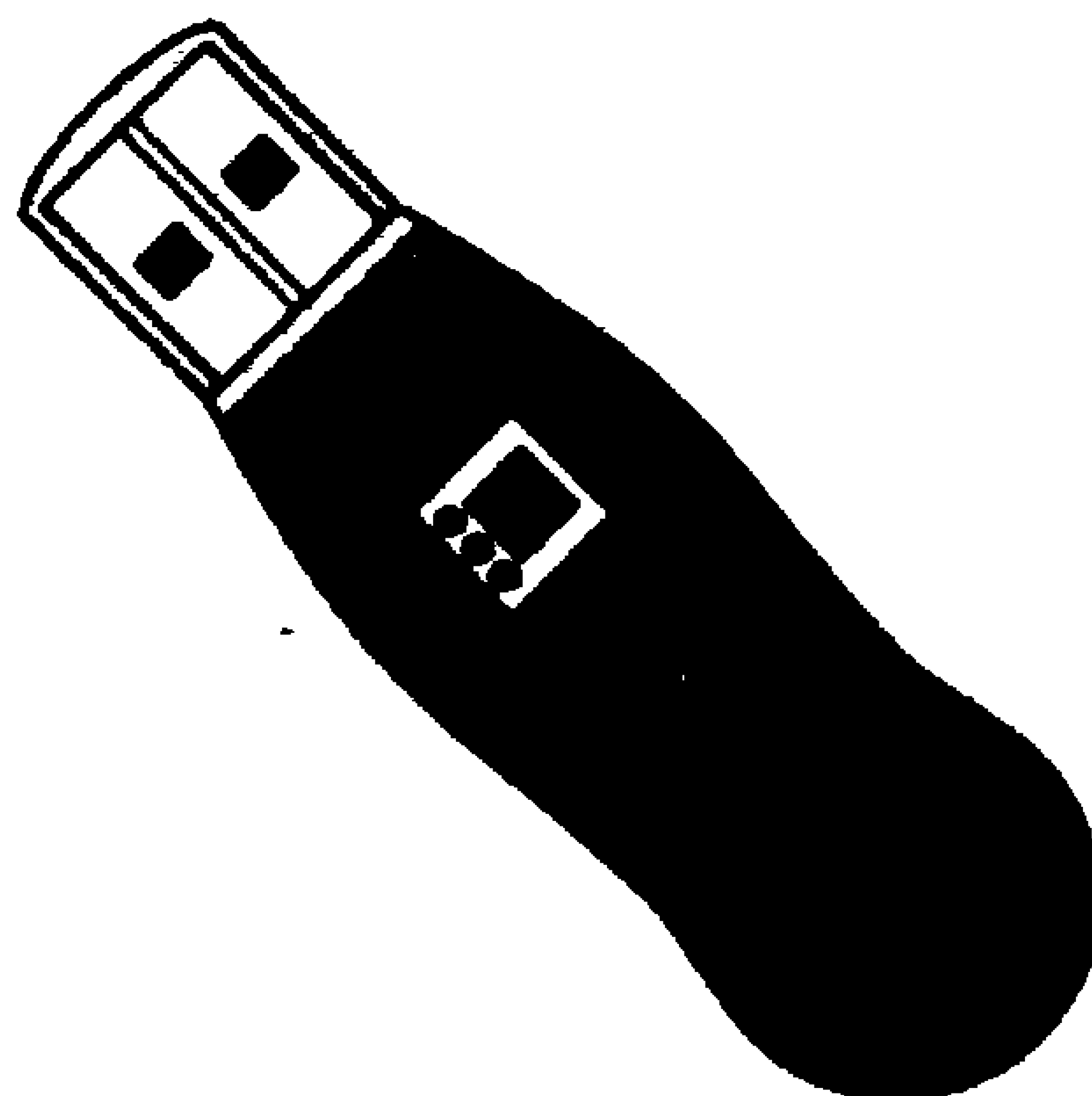
في حال صادفت بطاقة ذاكرة ومضية خلال أحد أعمال الحقيبة السوداء وأردت نسخ المحتويات إلى القرص الصلب، تزود بقارئ وناسخ البطاقات FlashGo لشركة Imation (www.imation.com). حيث يدعم جهاز USB المحمول تنسيقات CompaqFlash (النوع I و II)، SmartMedia، Multimedia Card، Secure Digital، و Memory Stick، سعره حوالي 55 دولاراً أمريكياً. ركّب في البداية بطاقة الذاكرة في قارئ البطاقة الصغير المحمول، ومن ثم ركّب القارئ إلى منفذ USB وابدأ بعملية النسخ.

ظهر منتج تخزين آخر معتمد على الذاكرة الومضية وهو محرك USB ومضي (USB Flash Drive) (انظر الشكل 1-7). وهو عبارة عن جهاز ذاكرة صغير، أكبر بقليل من حجم إبهامك، والذي يركّب في منفذ USB. ما عليك إلا وصل الجهاز، في أنظمة التشغيل Windows ME/2000/XP، والبدء بالنسخ (تأكد من وجود قرص برنامج التشغيل لتستخدمه للإصدارات الأقدم من نظام التشغيل Windows).

تتواجد محركات الذاكرة الومضية بالألوان الزاهية مع بعض النماذج التي تبدو مثل قلم تخطيط وأخرى مصممة كعلاقة مفاتيح. نتيجة لمظهرها غير الملفت للنظر وكونها جديدة في الأسواق، يمكن أن تمرر هذه الأجهزة دون أن تلاحظ في حال تم كشفك بأعمال التجسس. (إذا كنت مبدعاً وبارعاً في الأدوات الصغيرة، يمكنك إخراج محرك الذاكرة الومضية من غطائه ووضعه في شيء غير بارز مثل قلم تخطيط عريض، لتكون أكثر خداعاً).

تتراوح السعة التخزينية حالياً من 8MB إلى 512MB، كما تعتمد الأسعار على السعة (من 40 إلى 260 دولاراً أمريكياً). معدل النقل حوالي 1MBps، مع وجود بعض الأنواع الجديدة الخاصة بالمنفذ USB 2.0 تصل سرعات الكتابة إلى 4.5MBps.

يمكنك الحصول على لائحة من مختلف أنواع محركات الذاكرة الومضية، اتبع الرابط www.everythingusb.com/hardware/Storage/USB_Flash_Drives.htm.



الشكل (7-1) JumpDrive 2.0 Pro لشركة Lexar (www.lexarmedia.com)، محرك ذاكرة ومضية سعة تخزينه 256MB ومعدل النقل 4.8MBps. ما عليك إلا تركيب الجهاز إلى منفذ USB وتبدأ بنسخ الملفات.

وسائل التجارة: هجوم أجهزة iPod

نشرت جريدة **Wired News**، في شهر شباط (فبراير) عام 2002، مقالة حول حادثة وقعت في **Dallas**، من ولاية **Texas**. حيث قام مراهق كان يستمع إلى جهاز **Apple iPod** (وهو عبارة عن مسجلة محمولة تعزف ملفات صوتية من نمط MP3 مأخوذة من قرص مضغوط أو محمّلة من الإنترنت) بربط الجهاز إلى أحد حواسب **Macintosh** الخاصة بالمتجر. شاهد أحد الزبائن المراهق وهو يقوم بنسخ الإصدار الجديد لبرنامج **Microsoft Office** لنظام التشغيل ما إلى جهاز **iPod** (www.apple.com/ipod). حيث استطاع المراهق باستخدام اتصال **FireWire** نسخ منتج حجمه **200MB** في أقل من دقيقة إلى جهاز **iPod**.

مع أن هذه الحالة عبارة عن قضية واضحة لقرصنة البرمجيات مع السرقة أيضاً، إلا أنها تشير إلى جهاز **iPod** (وتوجد منه أنواع ذات الأحجام 5GB، 10GB، و 20GB ويظهر في الإعلانات أنه بالإمكان تحميل قرص مضغوط كامل في أقل من 15 ثانية)، يمكن أن يستخدم لإنجاز أعمال الحقيبة السوداء على الحواسب الشخصية وحواسب **Macintosh** باستخدام بطاقات **FireWire**.

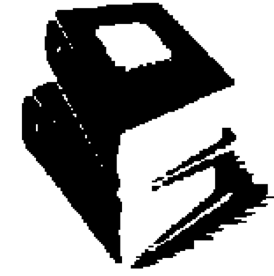
توجد منتجات مماثلة أخرى تعمل على الحواسب الشخصية، مثل **Creative Labs Nomad Jukebox Zen** (www.nomadworld.com/products/Jukebox_Zen/). تتوعد هذه الأجهزة الجديدة المتوافقة مع نظام التشغيل **Windows** والتي توصل إلى منفذ **USB** بوعود تحسسية كبيرة، حتى الجهاز **Zen** يملك خياراً للميكرفون من أجل القيام بالتنصت السمعي للتسجيل الرقمي.

قد تكون مسجلات MP3 التي توصل إلى منافذ USB وتدعم نسخ الملفات إلى المسجلة، أداة مثالية للجاسوس.

الأقراص الصلبة Hard Drives

ظهر أول قرص صلب عام 1957 كجزء من الحاسب الرئيسي التابع لشركة IBM (RAMAC 350). تضمن 50 قرصاً قياس كل منها 24 بوصة والتي استطاعت تخزين 5MB من البيانات فقط، وبلغت كلفة استئجاره سنوياً 35,000 دولار أمريكي. أما الآن أصبحت سعة الأقراص الصلبة أكثر من 100GB وانخفضت الأسعار لتصل إلى أقل من دولار واحد لكل 1GB.

شاعت أيضاً مضاعفة القرص الصلب في أعمال الفحوصات الشرعية الحاسبية، وفي أعمال التجسس أحياناً. لإجراء عملية المضاعفة، افتح غطاء الصندوق وركّب قرص صلب ثانوي فارغ إلى القرص الصلب الرئيسي الداخلي، ثم أقلع الحاسب باستخدام قرص لبرنامج المضاعفة وانسخ المحتويات الكاملة للقرص الرئيسي إلى القرص الثانوي، ليس عليك أن تقلق حول تجاوز مربع تسجيل الدخول الخاص بنظام التشغيل Windows. بعد انتهائك أعد كل شيء إلى مكانه وخذ القرص الثانوي إلى مكان آمن لإجراء عملية التحليل.



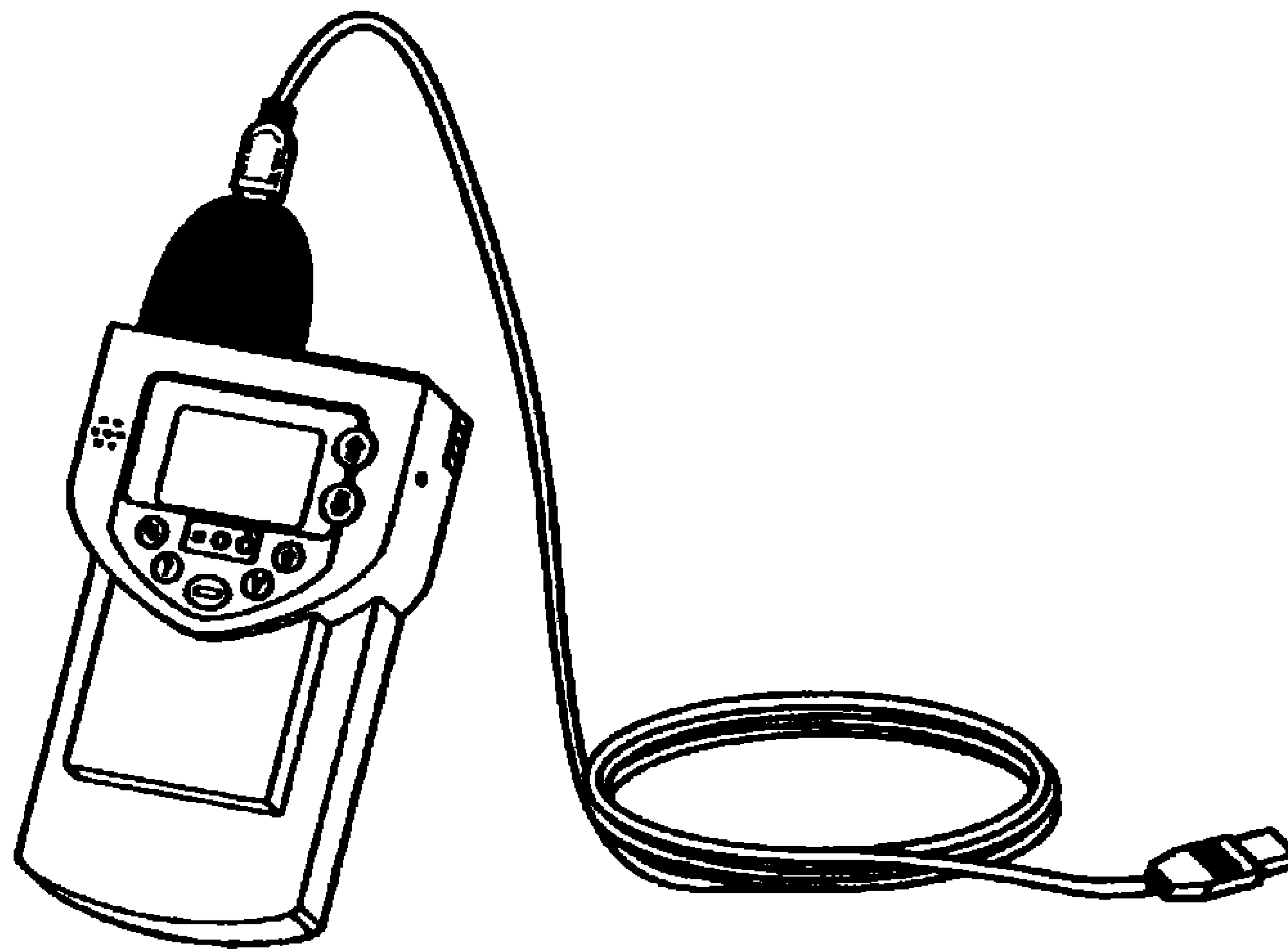
تمت مناقشة برمجيات المضاعفة الشرعية للقرص الصلب في الفصل الخامس.

يصل معدل نقل البيانات للقرص الصلب الداخلي التقليدي، وخاصة النماذج الأسرع ذات 7200 دورة في الدقيقة مع تخزين البيانات، إلى سرعة 100MBps. لكن عليك أيضاً حساب الزمن اللازم لفتح صندوق الحاسب الهدف، تركيب القرص الجديد، إنجاز عملية النسخ الفعلية، إزالة القرص الصلب الجديد، وتنظيف المكان ثانية. إذا لم تكن تملك الوقت الكافي خلال عمل الحقيبة السوداء، قد لا يكون استخدام محركاً داخلياً لإجراء النسخ خياراً جيداً. تشكل المحركات الخارجية مثل الأقراص الصلبة التي تتصل بمنفذ USB ومحركات الأقراص الصغرية Microdrives بديلاً أفضل بكثير.

وسائل التجارة: ناسخات أقراص التجهيزات

يشكل جهاز SF-500 من شركة Logicube أحد الأدوات المفضلة لمضاعفة الأقراص الصلبة لدى مكتب التحقيقات الفدرالي (والوكالات الأخرى الحكومية والاستخباراتية) (انظر الشكل 2-7). قم

بتوصيل القرص الصلب المصدر والقرص الصلب الفارغ الوجهة إلى الوحدة، وسوف تقوم بنسخ محتويات القرص المصدر إلى القرص الوجهة. لقد استخدم مكتب التحقيقات الفدرالي هذه الأجهزة مئات المرات خلال السنوات المنصرمة ويفضّلها لأنها سريعة، محمولة، وسهلة الاستخدام. (هذه الوحدات تعمل بشكل رائع مع محركات إلكترونيات الأجهزة المتكاملة IDE، إلا أن سرعتها تنخفض بشكل واضح عندما تستخدم مع محركات SCSI). الكلفة الأساسية لناسخ محمول 1,199 دولاراً أمريكياً (المجموعة الكاملة مسعرة 2,249 دولاراً أمريكياً)، يمكنك الحصول على مزيد من المعلومات من خلال الموقع www.logicube.com.



الشكل (7-2) ناسخ قرص صلب محمول من طراز SF-5000 من شركة Logicube مع وصلة USB، وهو المفضل لدى مكتب التحقيقات الفدرالي والوكالات الحكومية الأخرى.

توجد ناسخات أقراص صلبة أخرى، شائعة أيضاً لدى وكالات قوى القانون (ويمكن استخدامها بالطبع لنشاطات أقل شرعية) وهي:

- **Corporate Systems Portable Pro Drive:** تدعم وحدة Corporate Systems نسخ محركات الحواسب المحمولة بما فيها IDE، SCSI، SCA، و"2.5، مع العلم أن جهاز Logicube أسرع عند نسخ محركات IDE. وهو ليس صغير الحجم مثل سابقه ويأتي ضمن حقيبة كبيرة الحجم، لكنه مفضل من قبل الكثير من أعمال الفحوصات الشرعية الحاسبية، ومسعّر بقيمة 995 دولار أمريكي. لمزيد من المعلومات اتبع الرابط www.corpsys.com.
- **Intelligent Computer Solutions Image Masster Solo-2:** وهو عبارة عن ناسخ محمول آخر شبيه جداً بوحدة Logicube. تشير التقارير في هذا المجال أن Solo-2 يتعامل بصورة جيدة مع القطاعات التالفة، وهو أمر قد يعترض عمل بعض أجهزة النسخ الأخرى.

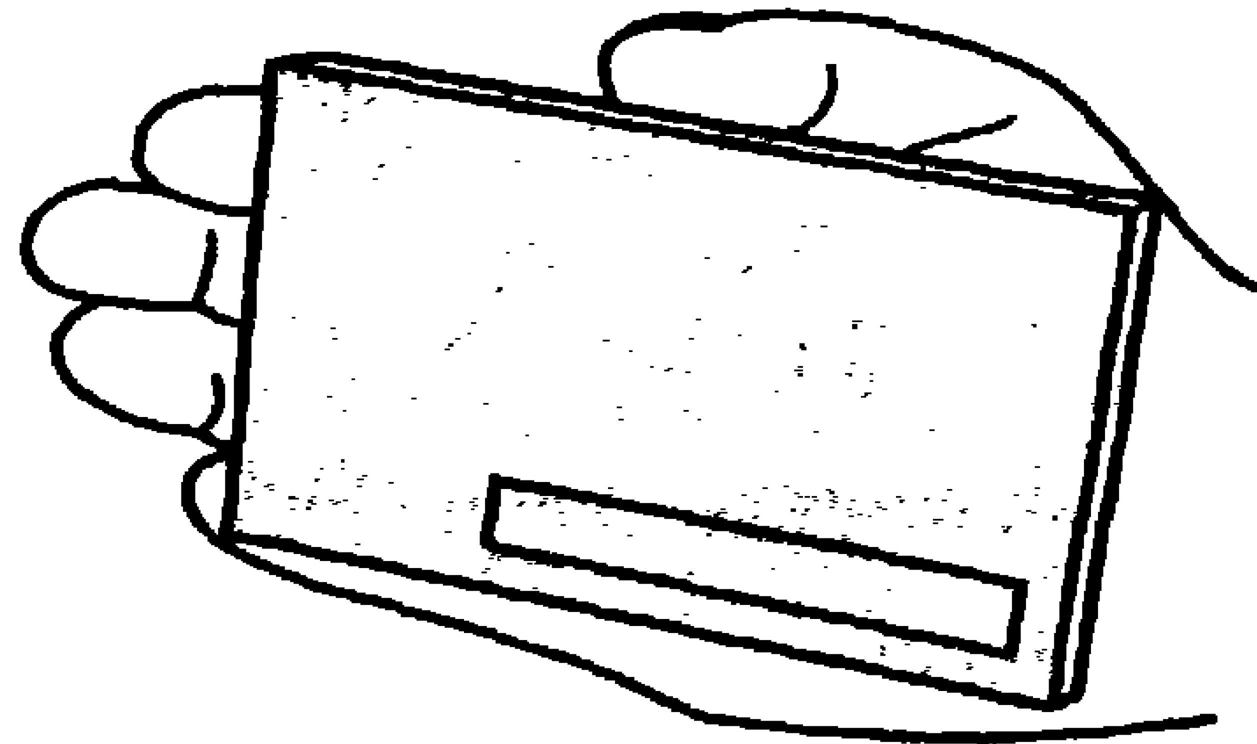
التكلفة الأساسية لهذه الوحدة 1,495 دولار أمريكي، ولمزيد من المعلومات اتبع الرابط .www.ics-iq.com

بالرغم من أن هذه الأجهزة مناسبة جداً لعملية المضاعفة، إلا أنه يمكنك أيضاً استخدام حاسب محمول وبرنامج مثل Linux dd Command، أو Norton Ghost للحصول على نفس النتيجة.

الأقراص الصلبة التي تتصل بمنفذ USB

تشكل الأقراص الصلبة التي تتصل بمنفذ USB (ومنفذ IEEE 1394) أدوات ممتازة لنسخ البيانات. حيث يمكنك بدلاً من أن تفك الحاسب الهدف وتركب محركاً داخلياً مؤقتاً من أجل نسخ البيانات، أن توصل محرك الأقراص الخارجي إلى منفذ USB وأن تبدأ بمضاعفة الملفات (معدلات النقل أبطأ من المحرك الداخلي لأن الجهاز محدود بالسرعة الأعظمية لمعالجة المعلومات لمنفذ USB). يوجد نوعان من هذه المحركات:

- **القياسي Standard**: مع أن هذه الأجهزة محمولة ويمكن استخدامها للتجسس، إلا أنها لن تتسع في جيبك (وخاصة مع محول التيار المتناوب وسلك الطاقة). يخزن القرص الصلب ما بين 20GB إلى 200GB من البيانات، وتتراوح أسعاره بين 100 إلى 250 دولار أمريكي.
- **المضغوط Compact**: محركات صغيرة يمكن أن تتسع بسهولة في الجيب وتخزن ما بين 5GB و 60GB من البيانات (انظر الشكل 3-7). تسحب هذه الأقراص الكهرباء من منفذ USB وبالتالي لا تحتاج إلى مصدر طاقة، تتراوح أسعارها بين 175 و 400 دولار أمريكي.



الشكل (3-7) قرص صلب USB من شركة Pockey Datastor (www.pocketec.net)، يتسع على راحة اليد بسهولة ويزن 2.5 كغ فقط أداة سرية مثالية لنسخ كميات كبيرة من البيانات.

محركات الأقراص الصغرية Microdrives

إذا كان هدفك حاسب محمول أو حاسب مكتبي مع قارئ بطاقات PC، يمكنك التفكير باستخدام محرك أقراص صغري Microdrive. محرك الأقراص الصغري هو بطاقة PC ذات قرص صلب مدمج، بوصة واحدة، وسعة تخزينه 340MB، 500MB، 1GB، أو 4GB (تختلف باختلاف الطراز). يمكن تركيب المحرك على أي منفذ يتوافق مع CompactFlash CF+Type II أو يتوافق مع منفذ بطاقات PC، ويصل معدل النقل إلى ما يقارب 40 إلى 60Mbps. تكلفة المحرك ذو السعة 1GB هي 350 دولار أمريكي. وقد اشترت شركة Hitachi أعمال شركة IBM المتعلقة بالأقراص الصلبة في نهاية عام 2002، وتقوم حالياً بتصنيع وتسويق محركات الأقراص الصغرية Microdrives. لمزيد من المعلومات اتبع الرابط www.hgst.com/products/microdrive/index.html.

أنظمة الشريط الاحتياطية Tape Backup Systems

يشيع استخدام أنظمة الشريط في الإعدادات المشتركة من أجل نسخ البيانات احتياطياً، وبالرغم من وجود نماذج محمولة، إلا أنها غير مناسبة لأهداف التجسس (فيما عدا نسخ الأدلة في مختبر الفحوصات الشرعية). أنظمة الشريط بطيئة بالمقارنة مع أجهزة التخزين الأخرى وتحتاج لتغيير الشريط بشكل متكرر. إذا صادفت نظام شريط احتياطي على الحاسب الهدف، استخدم بعض وسائط التخزين الأخرى لنسخ الملفات، وإذا وجدت شرطان نسخ احتياطي وقررت أخذها، تأكد من معرفة ما هي أنواع التجهيزات والبرمجيات المستخدمة لتحاول استرجاع البيانات فيما بعد.

أساليب أخرى لنسخ البيانات

لا تقيد نفسك باستخدام الأقراص المرنة، الأقراص المضغوطة، الأقراص الصلبة، وأجهزة الذاكرة واعتبارها الأسلوب الوحيد لنسخ البيانات. يملك الجاسوس الجيد دوماً الأداة المناسبة لعمله، وهناك عدة وسائل بديلة لنسخ البيانات التي يمكن أن تستخدمها.

نقل البيانات عبر الشبكة

إذا كان الحاسب الهدف متصلاً بشبكة (مثل شبكة الإنترنت) بإمكانك إرسال البيانات إلى حاسب آخر متصل بالشبكة بدلاً من نقل البيانات إلى جهاز تخزين محلي. لاحظ ما يلي:

- يعتمد معدل نقل البيانات كلياً على سرعة الاتصال الشبكي. قد يعرضك الاتصال البطيء لأن تنتظر الانتهاء من إيداع البيانات *(إيداع upload: في الاتصالات، عملية نقل نسخة من مجموعة من الملفات من الحاسب المحلي إلى حاسب آخر بعيد باستخدام مودم أو شبكة).
- قد تتم مراقبة اتصالات الشبكة، ومن المحتمل أن تترك دليلاً للاقتحام. على الأقل تأكد من أن الوجهة التي ترسل إليها البيانات ليست عنوان IP الذي يمكن أن يقود إليك.

إذا كانت الظروف ملائمة لنسخ البيانات من شبكة، هناك ثلاثة خيارات:

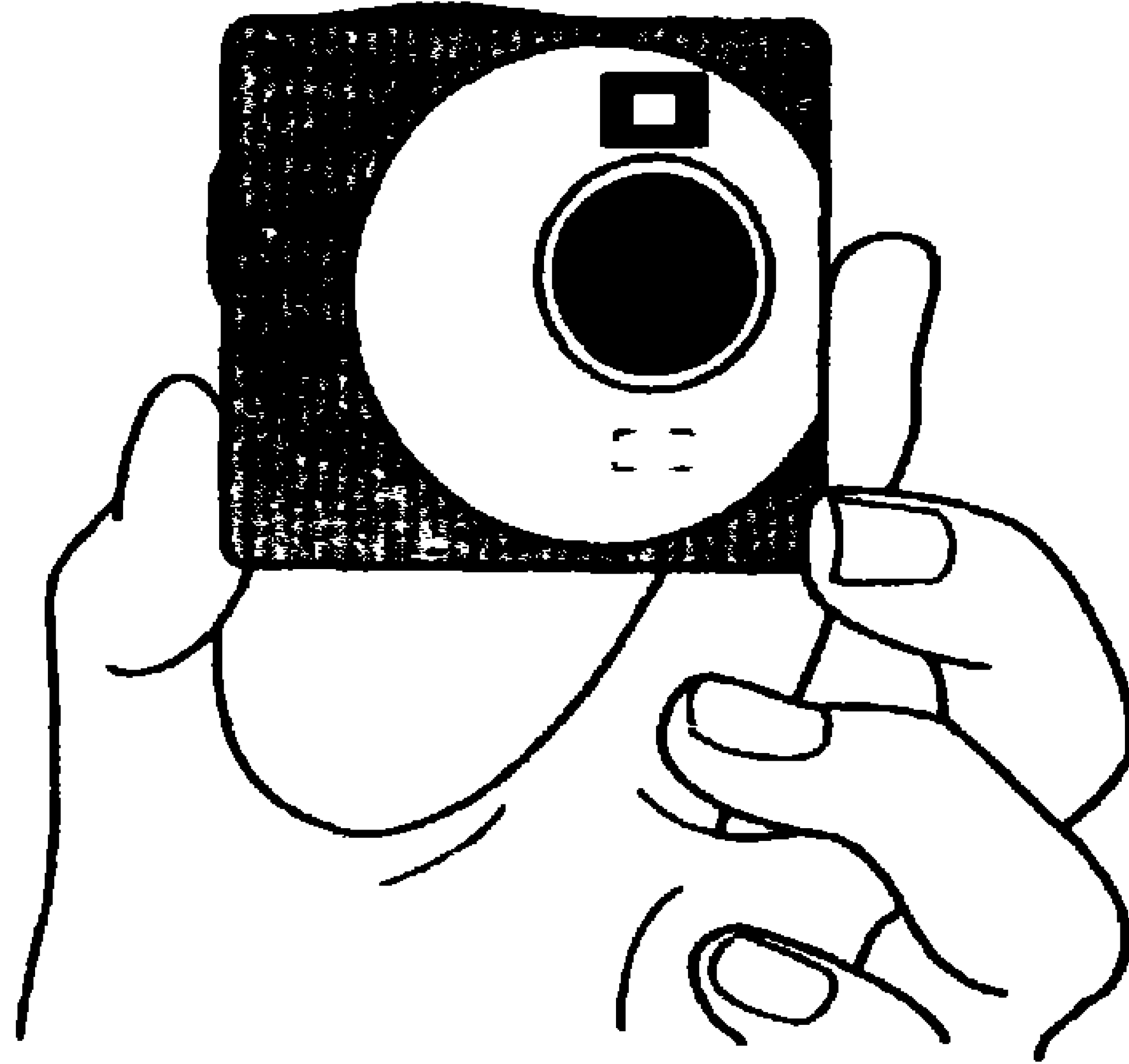
- **FTP، Telnet، وSSH**: إذا كنت تملك الوصول إلى حساب يدعم FTP، Telnet، أوSSH، بإمكانك دوماً الاتصال بهذا الحساب ومن ثم نسخ الملفات المحلية إلى الحاسب البعيد. (يجب أن تحمل معك تطبيقات مناسبة للعميل على قرص البرامج الذي بحوزتك).
- **البريد الإلكتروني E-mail**: إذا كنت تملك الوصول إلى البريد الإلكتروني العميل على الحاسب الهدف، يمكنك ببساطة إرسال ملفات مرفقة إلى حساب جاهز للبريد الإلكتروني قمت بإنشائه من قبل. يمكن استخدام هذه الطريقة مع كميات صغيرة من البيانات لكنها قد تتجاوز حدود حجم البريد الإلكتروني إذا حاولت إرسال ملفات مرفقة ذات حجم كبير.
- **NetCat**: سكين الجيش السويسري، وهي أداة سطر الأوامر التي يجب أن يملكها كل جاسوس. طورت هذه الأداة من قبل شخص يدعى Hobbit وأطلقت أول مرة عام 1995. تستطيع باستخدام هذه الأداة نقل، فحص، نسخ الملفات، تنفيذ الأوامر عن بعد، وإنجاز جميع أنواع نشاطات الشبكة المفيدة الأخرى. من أجل نسخ الملفات إلى حاسب بعيد تأكد أن برنامج NetCat يعمل عليه، ثم شغل البرنامج على الحاسب المصدر، حدد عنوان IP وانقل رقم الوجهة، وسوف تكون جاهزاً لنسخ الملفات. تتوفر نسخ مجانية لهذه الأداة الرائجة لأنظمة التشغيل Linux و Windows ، على الرابط www.atstake.com/research/tools/network_utilities/. (تتوفر نسخة معدلة لهذه الأداة Cryptcat، والتي تقوم بتشفير البيانات باستخدام خوارزمية Twofish، على الرابط www.farm9.org/Cryptcat/GetCryptcat.php).

الكاميرات الرقمية Digital Cameras

كل جاسوس حاسبي يجب أن يملك كاميرا من بين أدواته، الكاميرات أدوات أساسية لالتقاط الصور لمعلومات بالغة الدقة والتي لا تكون بتنسيق رقمي حيث يمكن نسخها بسهولة. كما لا يمكن الاستغناء عنها خلال أعمال الحقيبة السوداء وذلك لتوثيق الغرفة، لتتأكد أن كل شيء عاد لمكانه كما كان.

الكاميرا المثالية للجاسوس هي التحفة الصغيرة من شركة Minox (لمزيد من المعلومات اتبع الرابط www.minox-web.de). لقد ظهرت هذه الكاميرا منذ عام 1930 وما تزال رائجة حتى الآن بين الكثير من وكالات الاستخبارات حول العالم، وهي كاميرا صغيرة جداً، وزنها 56 غرام، وتلتقط صور مستخدمة فلماً ذو الأبعاد 8 x 11 mm.

كاميرا Minox تقليدية، أما الكاميرات الرقمية فهي متعددة الاستعمالات وأفضل للاستخدام. مع أنه يمكنك استخدام طرازاً تقليدياً كبيراً، إلا أنه هناك عدد متزايد من النماذج المختلفة والتي تتميز بنوعية الصورة، وميزات حجم الصورة. بعض الكاميرات مثل SiPix StyleCam Snap (www.sipixdigital.com)، انظر الشكل (7-4)، و Creative Labs Cardcam (www.americas.creative.com) يمكن أن تتسع على راحة يدك، ويمكن إخفاءها بسهولة، وغير مكلفة (حوالي 40 دولاراً أمريكياً و 80 دولاراً أمريكياً بالترتيب). بالرغم من أنها لا تملك شاشات عرض بلورية، فلاش، عدسة تكبير، أو تصور صوراً دقيقة حيث يمكن أن تتوقع مثل هذه الميزات في كاميرا مكلفة أكثر، إلا أنها تؤدي عملاً جيداً للكثير من تطبيقات التجسس.



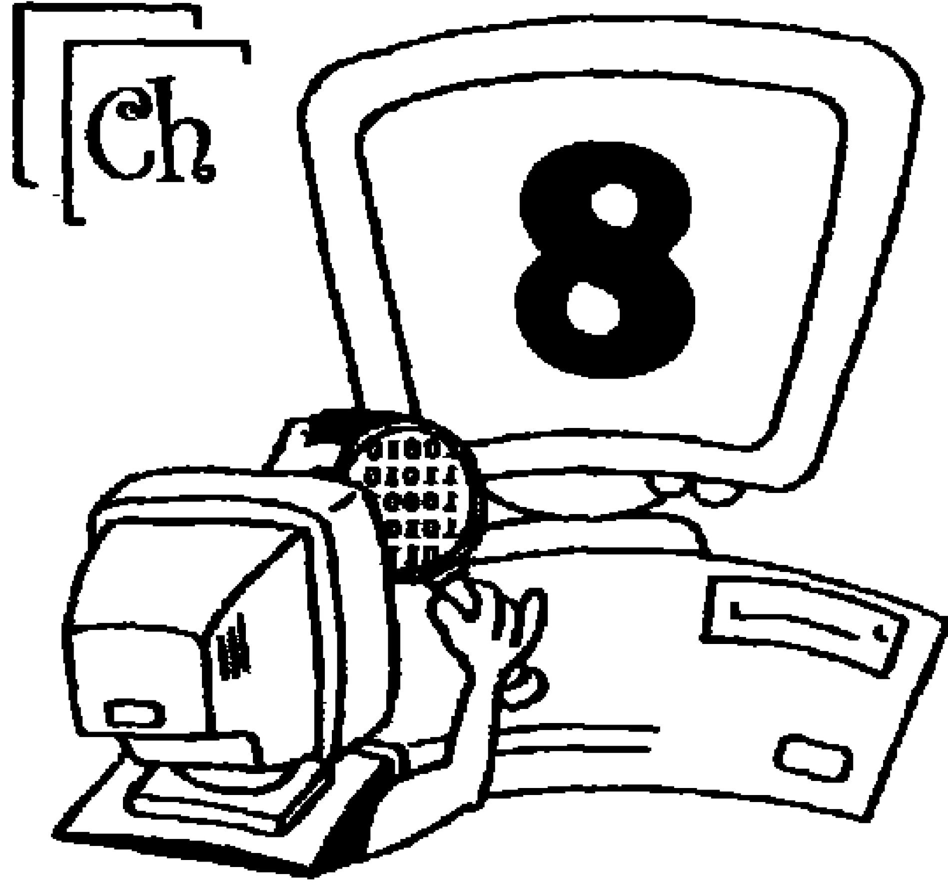
الشكل (7-4) كاميرا SiPix StyleCam Snap الرقمية، غير مكلفة، قابلة للإخفاء، وتزن أقل من كف واحد.

ملخص

هناك العديد من الخيارات لنسخ الملفات من الحواسب الهدف، وتتنوع هذه الأجهزة من حيث السرعة وقابلية الإخفاء. الأمر الأول الذي ستفكر به عندما تقوم بمضاعفة البيانات، هو الفترة الزمنية اللازمة لنسخ البيانات التي تهمك، ويحدد شرط الوقت نوع وسط التخزين الذي سيكون

بمقدورك أن تستخدمه وكمية البيانات التي سوف تستطيع نسخها بفعالية. عليك التدرّب على جهاز التخزين الذي تريد استخدامه، قبل أن تقوم بمضاعفة أي بيانات سواء كانت مضاعفة القرص الصلب كاملاً في مختبر للفحوصات الشرعية أو نسخ خطة عمل منافسك بشكل سري. سوف تجعل جلسات التدريب هذه العملية مألوفة بالنسبة لك (وتحدد أي خلل كامن) وتعطيك فكرة عن الفترة الزمنية التي سوف يستغرقها نسخ الملفات.

من جانب آخر، يشكل الأمن الفيزيائي مفتاح الدفاع ضد نسخ البيانات المحظور. ومن الواضح أنه كلما صعّبت الأمر على الجاسوس للوصول على الحاسب، زادت فرص حمايتك للمعلومات الهامة. الوقت هو في جانبك، وهو يربط بشكل مباشر بين كمية البيانات التي يمكن نسخها، وبالتالي إذا تمكنت من تخفيض الزمن الذي يستطيع الجاسوس قضاءه أمام الحاسب، تكون قد قلصت كمية البيانات التي يمكنه نسخها. أنظمة الإنذار، كاميرات المراقبة، والحراس الذين يجولون حول المبنى بانتظام هي بعض طرق الحماية التي يمكن أن تحد من نشاطات الجاسوس. اعتبار الوقت كإجراء مضاد يكون جيداً عند نسخ كمية كبيرة من البيانات، لكن يتم نسخ بعض المستندات الهامة في غضون ثوان. وهنا تأتي أهمية التشفير والذي يلعب دوراً مصيرياً في جدار الحماية لديك. حتى لو نجح الجاسوس في نسخ البيانات، إذا استخدمت تشفير قوي للحماية (واتّبعت سياسة قوية لكلمات المرور)، هناك فرصة كبيرة أن الجاسوس لن يتمكن من كشف معلوماتك الحرجة.



التطفل باستخدام مسجلات المفاتيح

مقدمة إلى مسجلات المفاتيح

مسجل المفاتيح هو برنامج أو جهاز يقوم بتسجيل المفاتيح التي تضغطها على لوحة المفاتيح. حيث يمكن أن تكشف مجموعة المفاتيح المضغوطة لكلمة مرور، دليلاً لعلاقة مشوهة، أو أية معلومات أخرى تفضّل إبعادها عن الناس. بالتأكيد فإن مفهوم التجسس على المفاتيح ليس جديداً، حيث استمرت مراقبة لوحات المفاتيح بشكل أو بآخر، وبدأت عندما قام E. Remington وأبنائه ببيع الآلة الكاتبة الأولى عام 1874. فيما يلي بعض الأمثلة حول التجسس على لوحات المفاتيح:

- بما أن الآلات الكاتبة تستخدم الأشرطة الحبرية، بالتالي تظهر جميع الحروف المكتوبة على الشريط. وفي بداية القرن العشرين، كانت وكالات قوى القانون ووكالات الاستخبارات تبحث دوماً عن الأشرطة المرمية في القمامة. حتى في التسعينيات، استخدم مكتب التحقيقات الفدرالي الأشرطة كجزء من الدليل لإدانة العميل الروسي المزدوج Aldrich Ames.
- يتضمن غلاف الكتاب "Inside the Company: CIA Diary"، الذي ألفه العميل السابق لوكالة الاستخبارات المركزية Phillip Agee CIA، صورة لآلة كاتبة محمولة تمت مراقبتها بشكل سري. قام صديق مزعوم للمؤلف منتسب إلى الوكالة، خلال السبعينيات من القرن الماضي، بإعارة العميل السابق Agee الآلة الكاتبة لكي تستطيع وكالة الاستخبارات المركزية مراقبة Agee بينما كان يؤلف قصته.
- منحت شعبية الآلات الكاتبة الإلكترونية الجواسيس مصدر طاقة مركب داخلياً من أجل وصل أجهزة التنصت. ومع أن الآلات الكاتبة ذات الطراز Blickensderfer كانت موجودة منذ عام 1902، إلا أنه لم تصل إلى شعبيتها التجارية إلا في العشرينيات من القرن الماضي.

كان الطراز IBM Selectric، الذي ظهر عام 1960، هدفاً سهلاً للتنصت لأنه كان متداولاً جداً. حيث كان بمقدور الجاسوس أن يستبدل بسهولة النموذج العادي بالنموذج الذي تتم مراقبته، ولن تلاحظ السكرتيرة الفرق بينهما. (يمكن أن يتم التنصت على الآلات الكاتبة باستخدام ميكرفون لمراقبة الخصائص الصوتية لضربات المفاتيح أو باستخدام إلكترونيات تقوم بتسجيل المفتاح الذي تم ضغطه. يرسل جهاز إرسال صغير المعلومات إلى أقرب مستقبل راديو، حيث يتم تسجيل ضربات المفاتيح ومن ثم يتم إعادة سماعها مرة أخرى لاحقاً لإجراء التحليل).

- اكتشف موظفو الأمن، عام 1984، ثلاث عشرة آلة كاتبة من طراز IBM تمت مراقبتها في روسيا. حيث تم استخدام هذه الآلات الكاتبة في مناطق آمنة في سفارة الولايات المتحدة الأمريكية في موسكو، بالإضافة إلى القنصلية في لينيغراد. لقد كانت أجهزة المراقبة ترسل المعلومات للروس لعدة سنوات.

لننتقل الآن إلى الحاضر. بالرغم من أنه يمكن استخدام بعض التقنيات المستعملة لمراقبة الآلات الكاتبة للتنصت على لوحات المفاتيح، إلا أنه من الأسهل بكثير استخدام برمجيات وتجهيزات متخصصة. في الواقع، حصل منذ عدة سنوات مضت انفجار موضوعي لمسجلات المفاتيح المجانية والتجارية المتوفرة على شبكة الإنترنت. (يملك الكثير من بائعي مسجلات المفاتيح التجارية برامج مدمجة مع عدد من مواقع الويب الفريدة لتسويق منتجاقم).

يستخدم الرؤساء في العمل مسجلات المفاتيح للتجسس على الموظفين، ويستخدمها الأزواج لمراقبة بعضهم البعض، كما يستخدمها الأهل لمعرفة نشاطات أطفالهم، حتى مكتب التحقيقات الفدرالي يستخدم مسجلات المفاتيح لملاحقة المجرمين. إذا تمكن الجاسوس من الوصول الفيزيائي إلى الحاسب، تمثل مسجلات المفاتيح خياراً مفضلاً للعمل.

أساليب الجواسيس

هل أنت مستعد لتمثل دور الجاسوس مرة أخرى؟ جيد، سوف تكون مسجلات المفاتيح من أحد الأدوات الفعالة داخل حقيبتك السوداء.

توجد طريقتان لاستخدام مسجلات المفاتيح:

- **محلياً**: إذا كنت تملك الوصول الفيزيائي إلى الحاسب الهدف يمكنك تثبيت برنامج أو جهاز المراقبة. عليك أن تتأكد من أنه لديك الوقت الكافي لتكون وحدك مع الحاسب، حيث

يستغرق تثبيت مسجل المفاتيح البرمجي حوالي خمس دقائق، بينما يحتاج جهاز مسجل المفاتيح إلى دقيقة واحدة ليتم تركيبه.

- **عن بعد:** إذا لم تملك وصولاً فيزيائياً إلى الحاسب الهدف، أرسل رسالة إلكترونية إلى الهدف تتضمن حصان طروادة على شكل ملف مرفق. يوجد عدد من تطبيقات حصان طروادة والتي تتضمن مسجلات المفاتيح، بالإضافة إلى بعض مسجلات المفاتيح المعينة مصممة خصيصاً لهذا النوع من الهجوم. *(حصان طروادة: بشكل عام هو برنامج مدمر متنكر بشكل لعبة أو خدمة أو تطبيق ويؤدي إلى تلف نظام الحاسب عند تنفيذه).



لمزيد من المعلومات حول تطبيقات حصان طروادة وتطبيقات التحكم عن بعد، انتقل إلى الفصل التاسع.

طالما قمت بتثبيت مسجل المفاتيح، فإنه يقوم بمراقبة الحاسب الهدف ويقوم بتسجيل البيانات. والآن عليك الوصول إلى الحاسب فيزيائياً للحصول على النتائج، أو إذا كنت تستخدم مسجل مفاتيح متطور يمكنك أن تجعله يرسل نتائج المراقبة إليك مباشرة عن طريق البريد الإلكتروني. توجد أيضاً أنواع أخرى من مسجلات المفاتيح والتي تفتح منفذاً على الحاسب الهدف، حيث يمكن أن تصل إلى الحاسب مباشرة إذا كنت تملك عنوان IP الخاص به. لكن عليك توخي الحذر عند استخدام مسجل مفاتيح يرسل نتائج ضربات المفاتيح عن طريق شبكة الإنترنت، حيث يجب أن تغطي آثارك. و ليس من الذكاء أن يتم إرسال ملف السجل لضربات المفاتيح إلى حساب بريدك الإلكتروني الشخصي أو كشف عنوان IP لحاسبك عندما تتصل بالحاسب الهدف عن بعد للحصول على نتائج المراقبة.

استغلال نقاط الضعف

كل حاسب يستخدم لوحة المفاتيح كجهاز إدخال، معرّض لهجوم مسجل المفاتيح. لقد تم تطوير مسجلات مفاتيح برمجية لجميع أنظمة التشغيل الموجودة حالياً، وطالما يستخدم الناس لوحة المفاتيح لطباعة النصوص، يمكنك استخدام مسجل المفاتيح للتجسس عليهم. (وقبل أن تسأل عن برمجيات التعرّف على الأصوات، استخدم جهاز التسجيل التقليدي لتسجيل الكلام. تمت مناقشة أجهزة التنصت الصوتية باختصار في الفصل 12).

سوف نناقش الآن مبدأ عمل مسجلات المفاتيح البرمجية والصلبة ونعرض بعض ميزاتها العامة.

مبدأ عمل مسجلات المفاتيح البرمجية

مسجلات المفاتيح البرمجية بسيطة نسبياً - يكتب المبرمج شيفرة لاعتراض كل مفتاح مضغوط ومن ثم يسجل قيمة المفتاح إلى ملف التسجيل. توجد ثلاث طرق لإنشاء مسجل مفاتيح برمجي:

- **مسجلات المفاتيح منخفضة المستوى Low-Level keyloggers**: تم بناء هذه البرامج باستخدام اللغة assembly. تعمل باستخدام خطاف (واجهة تسمح للمبرمج أن يدخل شيفرة مخصصة) إلى مقاطعة لوحة المفاتيح (إشارة من التجهيزات التي تخبر عن حالة المفتاح) وتحويل الخرج إلى شيفرة مخصصة. يتم تسجيل كل مفتاح ومن ثم تستدعي الشيفرة المعالج الأصلي لتمرير المفتاح بشكل عادي.
- **مسجلات المفاتيح لواجهات برمجة التطبيقات في نظام التشغيل Operating System API keyloggers**: لقد سهّل نظام التشغيل Windows تطوير مسجلات المفاتيح كثيراً. حيث لا يحتاج الجاسوس إلى معلومات مفصلة عن البرمجة بلغة assembly والأمور المتعلقة بداخل النظام، بل يمكنه برمجة مسجل مفاتيح باستخدام أي لغة عالية المستوى. (توجد كمية كبيرة من الشيفرة المصدرية الخاصة بمسجلات المفاتيح المكتوبة بلغة البرمجة Visual Basic على شبكة الإنترنت، في الحقيقة أحد مسجلات المفاتيح التجارية المتداولة مكتوب بلغة البرمجة VB). يتحقق البرنامج الذي يعمل في الخلفية بصورة متكررة حالات المفاتيح ولمعرفة إذا تم ضغط المفتاح باستخدام أحد استدعاءات واجهة برمجة التطبيقات (API) GetAsyncKeyState و GetKeyState في نظام التشغيل Windows.

  كلما تم الضغط على مفتاح، يتم تسجيل القيمة المعادة. يستطيع مسجل المفاتيح أيضاً أن يستخدم واجهة برمجة التطبيقات SetWindowsHookEx لنظام التشغيل Windows لتتبع رسائل النظام ومعالجة أحداث لوحة المفاتيح باستخدام معالجات خاصة.
- **مسجلات المفاتيح لبرنامج تشغيل الجهاز Device Driver keyloggers**: وهي أكثر الأنواع خفية لأنها تعمل على أخفض مستوى من نظام التشغيل Windows. بالنسبة للحواسب التي تعمل على أنظمة التشغيل Windows 9x/ME، تمت برمجة مسجلات المفاتيح مثل برامج التشغيل الافتراضية للأجهزة (vxds.). أما بالنسبة للحواسب التي تعمل على الأنظمة Windows 2000/XP، تمت برمجة مسجلات المفاتيح مثل نموذج برنامج تشغيل Windows في نمط النواة Kernel، برامج تشغيل (WDM). *(النواة Kernel: القلب النابض لنظام التشغيل، وهو الجزء الذي يدير الذاكرة والملفات والأجهزة المحيطية، ويحافظ على التاريخ والزمن، ويربط بين التطبيقات، ويخصص موارد النظام). لا يوجد الكثير من مسجلات المفاتيح لبرنامج تشغيل الجهاز نتيجة للتعقيدات المرتبطة بكتابة برنامج تشغيل الجهاز مقارنة مع استدعاء إجرائية API.

لا يرغب معظم الجواسيس أن يكتشف الأشخاص المستهدفون أنه تتم مراقبتهم بوساطة مسجل مفاتيح، ولم تتم برمجة جميع مسجلات المفاتيح بشكل متماثل لتكون خفية. حيث يستخدم مسجل المفاتيح الجيد تقنيات متنوعة ليمنع المستخدم من اكتشافه. ومن بعض الأساليب الشائعة والماكرة لتجنب اكتشاف مسجل المفاتيح ما يلي:

- **الاختباء من مدير المهام:** توجد دالة kernel32.dll في الأنظمة Windows 9x/ME تسمى RegisterServiceProcess. كما يتوضح من الاسم، تسجل هذه الدالة العملية كخدمة تجعل العملية معفية من إيقاف التشغيل التلقائي عند تسجيل الخروج ولا تعرض العملية ضمن نافذة مدير المهام. تستخدم مسجلات المفاتيح الخفية هذه التقنية وتعمل في الأنظمة Windows 9x/ME (تظهر هذه العمليات المخفية في الأنظمة Windows NT/2000/XP، بسبب اختلاف التصميم). بينما تتفادى مسجلات المفاتيح التي تعمل مثل برامج التشغيل للأجهزة مشكلة الكشف من قبل مدير المهام ومستعرضات العمليات الأخرى.
- **استخدام اسم مزيف للعملية:** بالتأكيد سوف يؤدي استخدام الاسم EvilKeylogger إلى فضح مهمة العملية. بينما تحوي مسجلات المفاتيح الخفية اسم ملف واسم عملية مزيف لتجنب إثارة الشكوك.
- **استخدام أسماء ملفات وسجلات غامضة:** تحوي الملفات التي تكوّن جزءاً من تثبيت مسجل المفاتيح أسماء غامضة للملفات والسجلات ومصممة خصيصاً لتهدئة المستخدم غير الشكاك وذلك ليظن أن هذه الملفات هي جزء من نظام التشغيل. تقوم بعض مسجلات المفاتيح بإعادة تسمية الملفات بعد تشغيلها لتفادي الكشف اللاحق.
- **إخفاء ملفات السجل:** غالباً يتم تشفير ملفات السجل الخاصة بضربات المفاتيح لمنع المستخدم من اكتشاف محتوياتها. كما يمكن استخدام لواحق ملفات مزيفة مثل استعمال لاحقة ocx. لملف سجل نصي، مما يؤدي إلى اعتقاد مراقب عرضي أن الملف هو عنصر تحكم متخصص بكائنات OLE. كما تغير بعض مسجلات المفاتيح تواريخ ملفات السجل لمنع المستخدمين من البحث عن الملفات الجديدة أو المعدلة حديثاً.

يعتمد مستوى خفية مسجل المفاتيح على هدفك. حيث عليك استخدام مسجل مفاتيح سري لمستخدم متطور وشكاك، أما بالنسبة لفرد من العائلة يتمتع بثقافة حاسبية متوسطة فإنك لن تحتاج إلا إلى مسجل مفاتيح بسيط. عموماً تكون مسجلات المفاتيح التجارية خفية أكثر من الإصدارات المجانية المتوفرة على الإنترنت.

توفر مسجلات المفاتيح

بالتأكيد وجود مسجلات المفاتيح ليس سراً، مع أنها مصممة لتعمل بصورة خفية على الحاسب. لقد تلقت أدوات التنصت هذه تغطية شاملة ومكثفة من خلال وسائل الإعلام الشعبية والحاسبية، كما أنه يتم تسويق الإصدارات التجارية بصورة جيدة. يتم تحميل مسجلات المفاتيح بنقرة زر واحدة، حيث أظهر محرك البحث Google أكثر من 210,000 صفحة نتيجة للبحث عن الكلمة "keylogger" ومن ضمنها أربع روابط مضمونة إلى منتجات تجارية. عرضت بعض مواقع الويب التجسسية، في نهاية عام 2002، أكثر من 250 مسجل مفاتيح تجاري ومجاني. كما يدّعي المعلن عن برنامج SpyCop، وهو برنامج تجاري للكشف عن وجود مسجلات مفاتيح، أن البرنامج يستطيع أن يكشف عن وجود أكثر من 300 مسجل مفاتيح مختلف. يمكننا تشبيه مسجلات المفاتيح بالفيروسات حيث تظهر إصدارات جديدة دوماً بشكل دوري، وذلك بسبب توفر الشيفرة المصدرية للعامة واكتشاف تقنيات إخفاء جديدة وذلك لحجب مسجلات المفاتيح عن ضحاياها.

ما خلف المفاتيح - مسجلات متقدمة

كانت مهمة مسجلات المفاتيح الأولى تتلخص بمعنى اسمها تماماً وهو تسجيل ضربات المفاتيح، لكن تقوم الإصدارات الحالية لمسجلات المفاتيح المتطورة والحديثة وخاصة التجارية منها، بوظائف مراقبة إضافية إلى جانب تسجيل المفاتيح.

وفيما يلي بعض هذه الميزات:

- **التقاط محتويات الشاشة:** تستخدم بعض البرامج تقنيات أمنية مختلفة، منها استخدام لوحات مفاتيح افتراضية تظهر على شاشة الحاسب والمصممة خصيصاً للتغلب على مسجلات المفاتيح (حيث تظهر صورة للوحة المفاتيح على الشاشة وتنقر على المفاتيح باستخدام الفأرة لإدخال النص، وذلك لتجنب استخدام لوحة المفاتيح الفيزيائية). هناك نوع من مسجلات المفاتيح يقاوم هذا الإجراء المضاد وذلك عن طريق التقاط صور دورية للشاشة خلال أحد نشاطات البرنامج.
- **حفظ محتويات الحافظة:** يتم تسجيل جميع النصوص التي يتم إدخالها إلى الحافظة، حيث يؤدي فتح ملف نصي يحوي حسابات وكلمات مرور ونسخ النص ومن ثم لصقه إلى حقل الإدخال، إلى تجنب مسجلات المفاتيح البسيطة وذلك لأنه لم يتم ضغط أي مفتاح. بينما إذا تمت مراقبة الحافظة يتم تسجيل هذه المعلومات.

- **تسجيل المحتويات النصية للنافذة**: من الممكن أن تكون مراقبة طباعة المستخدم غير كافية وقد ترغب بالحصول على معلومات أكثر، مثلاً معرفة الجانب الآخر من محادثة تتم من خلال نافذة المحادثة الفورية عبر الإنترنت. وتقوم هذه الميزة بالتقاط النص الكامل الذي يظهر في النافذة.
- **عرض خرج كاميرا الويب**: إذا كانت هناك كاميرا ويب متصلة بالحاسب، يتم اعتراض وحفظ جميع ملفات الفيديو التي يستقبلها الحاسب من الكاميرا. قد يقوم شخص ما يبعد عنك آلاف الأميال بمراقبتك أو مراقبة أي شيء تشير إليه كاميرا الويب التي تخصك، دون أن تعلم.
- **تسجيل نشاطات الملفات**: يعرض مسجل المفاتيح جميع النشاطات المطبقة على الملفات، مثل نقل، إعادة تسمية، نسخ، أو حذف. تفيد هذه الميزة خلال عملية جمع الدليل.
- **عرض مواقع الويب التي قمت بزيارتها**: تزودك بعض المنتجات بقائمة مريحة لجميع مواقع الويب التي أدخلها المستخدم، بدلاً من القيام بعملية تفحص ضربات المفاتيح المملة.
- **توليد تقارير**. تحفظ الكثير من مسجلات المفاتيح الأدلة التي تم جمعها بتنسيق سهل القراءة والذي يمكن أن يحول إلى ورقة عمل أو قاعدة بيانات.
- **الوصول إلى المعلومات عن بعد**: ترسل بعض أنواع مسجلات المفاتيح المعلومات التي تم الحصول عليها عبر البريد الإلكتروني إلى عنوان محدد من قبل الجاسوس، بينما تستطيع أنواع أخرى الوصول إلى الحاسب الهدف من خلال شبكة محلية أو شبكة الإنترنت.

عندما تختار مسجل مفاتيح متطور، عليك أولاً تحديد النشاطات التي ترغب بمراقبتها، ولا تنجذب وراء ترويج التسويق إذا كانت حاجاتك تكفي لتستخدم مسجل مفاتيح يراقب ضربات المفاتيح فقط. لا تحتاج في كثير من الأوقات إلى جميع الميزات التي قد يقدمها البرنامج، ومن الأفضل أن تستخدم أداة غير مليئة بوظائف إضافية غير ضرورية.

أساليب: آفاق ما وراء كلمات المرور

إذا كنت تستخدم مسجل مفاتيح، لا تركّز كلياً على كلمات المرور فقط، الأسرار التجارية، أو الأدلة لنشاط غير قانوني. حيث يمكنك استخدام المعلومات التي حصلت عليها من مسجل المفاتيح مع بعض مهاجمات الهندسة الاجتماعية لكشف مزيد من المعلومات. لنفترض أنك اعترضت محتويات رسالة بريد إلكتروني موجهة من نائب الرئيس Frank Jordan إلى المهندسة Karla Knight. ويدور موضوع الرسالة حول إمكانية إطلاق ميزة جديدة للمكنسة الكهربائية

XP-9000. يا للهول! لقد حصلت على اسم المهندسة ومعلومات كافية عن المنتج لكي تتصل بها وتقول أنك تعمل مع Frank Jordan، ولديك بعض التساؤلات حول المنتج XP-9000.

مضبوط: Nicodermo Scarfo، الأصغر

اقتحم عملاء مكتب التحقيقات الفدرالي بشكل سري مكتب أعمال واقع في New Jersey، في شهر كانون الثاني (يناير) عام 1999، مالكه هو Nicodermo Scarfo، الأصغر، وهو ابن عضو عصابة Philadelphia المسجون، ويدعى "Nicky الصغير" Scarfo. لقد أصيب عملاء المكتب بالإحراج، بعد أن دخلوا إلى المكتب وبحوزتهم مذكرة تفتيش لنسخ محتويات الحاسب، عندما اكتشفوا في وقت لاحق أن أحد الملفات، تحت الاسم "Factors"، كانت محمية باستخدام برنامج التشفير PGP (Pretty Good Privacy).

ثم منح بعد ذلك قاضي المحكمة مذكرة ثانية لعملاء مكتب التحقيقات الفدرالي، ليقوموا بتثبيت مسجل مفاتيح بشكل سري على الحاسب بهدف انتزاع كلمة المرور التي استخدمها Scarfo لتشفير الملف المتوقع أن يحوي معلومات حول إنشاء السجلات ومنح قروض بفائدة كبيرة جداً. اقتحم العملاء مكتب أعمال Scarfo ثانية، في شهر أيار عام 1999، وقاموا بتثبيت أحد أنواع مسجلات المفاتيح على حاسبه. أدى مسجل المفاتيح مهمته خلال 14 يوماً وتم تسجيل عبارة المرور للبرنامج PGP. إلا أن عبارة المرور هذه لم تقم بفك تشفير الملف الأصلي، ووجد العملاء إصداراً أحدث للملف مشفر بعبارة المرور نفسها، وحصلوا على الدليل المطلوب لمحاكمة Scarfo الأصغر، لكن الحكاية لم تنته.

طالب محامي Scarfo تفاصيل حول مسجل المفاتيح، لكن لم يقبل مكتب التحقيقات الفدرالي كشف أية معلومات حوله، قائلين بأن هذا الأمر يتعلق بالأمن القومي. ثم تلقت القضية فجأة اهتماماً قومياً حول مسألة حقوق الخصوصية الشخصية الحاسبية مقابل حق قوى القانون في استخدام تقنيات سرية للتجسس الحاسبي. وافق القاضي في هذه القضية مع الحكومة بأن هذه التقنية كانت بالغة الدقة ليتم مشاركتها مع الجمهور، وأقر Scarfo بالتهم الموجهة إليه في ربيع عام 2002.

وفي نهاية الأمر، نشر مكتب التحقيقات الفدرالي معلومات قليلة حول مسجل المفاتيح في شهادة خطية متعلقة بالقضية، مشيراً إليه باسم KLS، أو Key Logger System.

- لقد تم ابتكار KLS خصيصاً لمكتب التحقيقات الفدرالي والذي يعد مالكه الشرعي، ويتألف من عدة مكونات (والتي قد تكون برمجيات، تجهيزات، برمجيات ثابتة[1]، أو الثلاثة معاً).

[1] البرمجيات الثابتة Firmware: الإجرائيات البرمجية المخزنة في ذاكرة ROM، والتي تبقى ثابتة حتى في غياب التغذية الكهربائية بعكس ذاكرة RAM.

- لا يقوم KLS بتسجيل ضربات المفاتيح عند استخدام المودم (كان Scarfo يملك حساباً على خدمة America Online). إذا تم استخدام المودم، وكان Scarfo يستخدم شبكة الإنترنت، سوف يتم تصنيف الحاسب كجهاز اتصال إلكتروني مما يتطلب أمراً إضافياً من المحكمة للتنصت.
- يبدو أن عملاء مكتب التحقيقات الفدرالي قد تجنبوا هذا الأمر وذلك بفحص نوافذ العمليات الجارية وتسجيل ضربات المفاتيح للبرامج التي لم تتفاعل مع المودم. وقد بحث البرنامج الذي كان يعمل في الخلفية، على الأغلب عن وجود نافذة برنامج PGP ومن ثم بدأ بتسجيل ضربات المفاتيح.
- تطلب الحصول على نتائج مسجل المفاتيح KLS وصولاً فيزيائياً للحاسب.، وقد نفذ عملاء المكتب خمس عمليات سرية إلى مكتب أعمال Scarfo. حيث تم وصف أربع محاولات من أصل خمس أن "الحاسب غير فعال أو غير موجود." (وهي عبارة غامضة تدعو للاعتقاد أن مكتب التحقيقات الفدرالي كان يراقب حاسباً محمولاً). كان الحاسب المحمول متواجداً مع صاحبه في عشية عيد جميع القديسين عام 1989 عندما نجا من محاولة اغتيال في المطعم. لكن، تفاخر Scarfo لأحد أصدقائه، في أحد المكالمات الهاتفية التي قام مكتب التحقيقات الفدرالي بتسجيلها في بدايات التحقيقات. " I got a monster. I got a f***ing DVD in there ... 128 megs of ram، a Pentium III، 450 ... a 19-inch monitor and .("Digital Surround Sound. The whole f***ing nine yards.

لم تتوفر المزيد من المعلومات حول مسجل المفاتيح KLS بعد ذلك الوقت، مع التفكير المستمر بحقيقة KLS.

ولمزيد من المعلومات، كانت كلمات مرور Scarfo "nds09813-050،" وهو رقم التعريف الخاص بوالده في السجن الفدرالي.

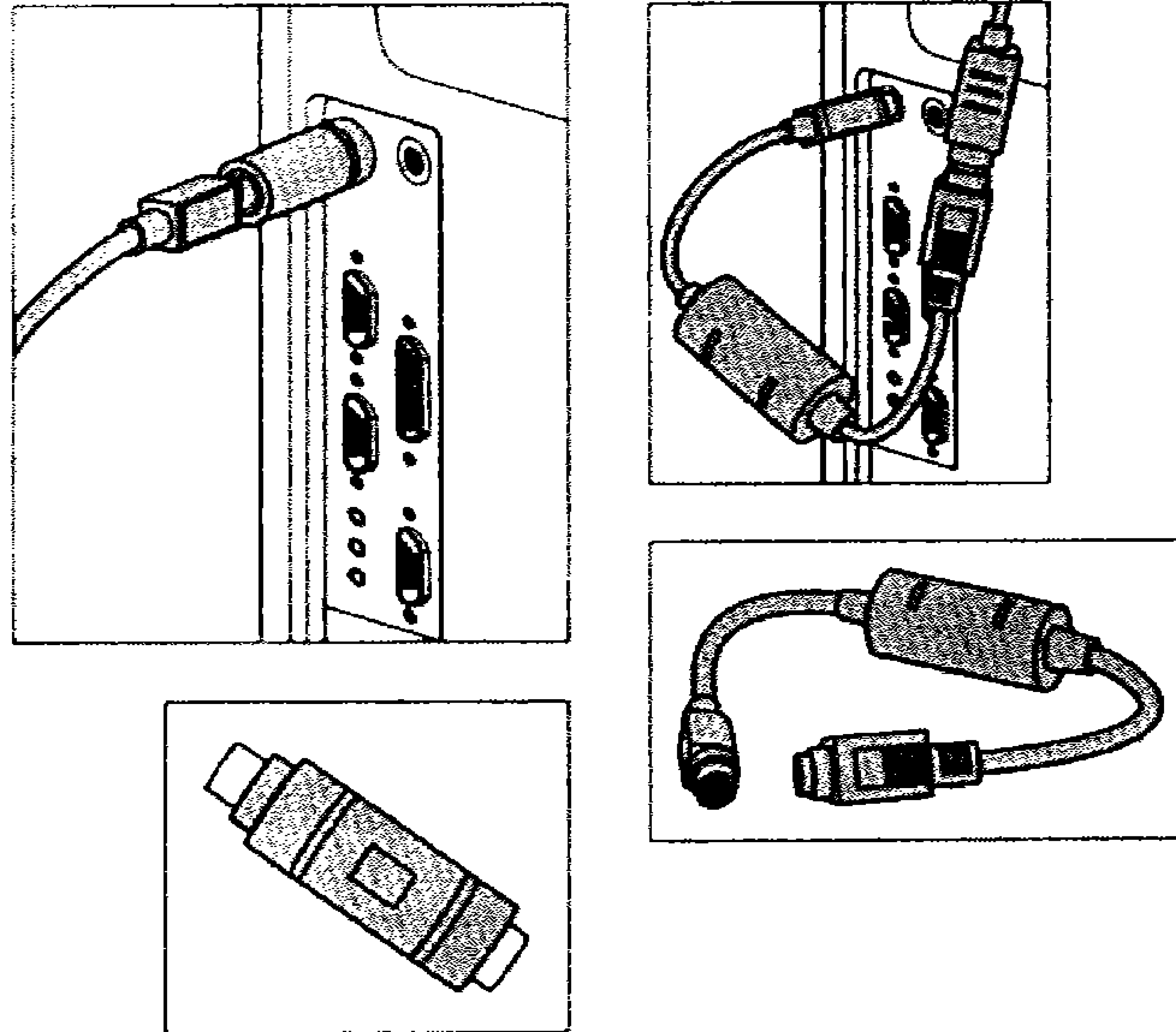
مبدأ عمل مسجلات المفاتيح الصلبة

وهو نوع آخر من مسجلات المفاتيح، تتألف هذه الأجهزة من أسلاك كهربائية إلكترونية تقوم بتسجيل ضربات المفاتيح عندما يتم إرسالها من لوحة المفاتيح إلى وحدة التحكم بلوحة المفاتيح في الحاسب (انظر الشكل 1-8). ما عليك سوى توصيل الجهاز فقط. تتم عملية الالتقاط بوساطة التجهيزات الصلبة ولا حاجة لوجود أية برمجيات (هذه مشكلة بالنسبة لهذا النوع من مسجلات المفاتيح لأنك تستطيع رؤية مسجل المفاتيح الموصول إلى منفذ لوحة المفاتيح).

هناك نوعان من مسجلات المفاتيح الصلبة التجارية:

- **مضمنة:** توصل مسجلات المفاتيح المضمنة إلى منفذ لوحة المفاتيح في الحاسب، ومن ثم يوصل سلك لوحة المفاتيح إلى مسجل المفاتيح. يبدو مسجل المفاتيح مثل سدادة الوصلة أو سلك يشبه السلك الموجود في المرشح الموازن الإلكتروني (انظر الشكل 8-1).
- **لوحة المفاتيح:** حيث تركب الأسلاك الكهربائية لتسجيل المفاتيح داخل لوحة المفاتيح نفسها. ومن الصعب جداً كشف هذا النوع من مسجلات المفاتيح، ما لم تفك لوحة المفاتيح (وتعرف عما تبحث).

تتضمن مسجلات المفاتيح الصلبة ذاكرة داخلية مدمجة تخزن ضربات المفاتيح عند إدخالها، وعندما تمتلئ الذاكرة يتم الكتابة فوق البيانات الأقدم واستبدالها بضربات المفاتيح الأحدث.



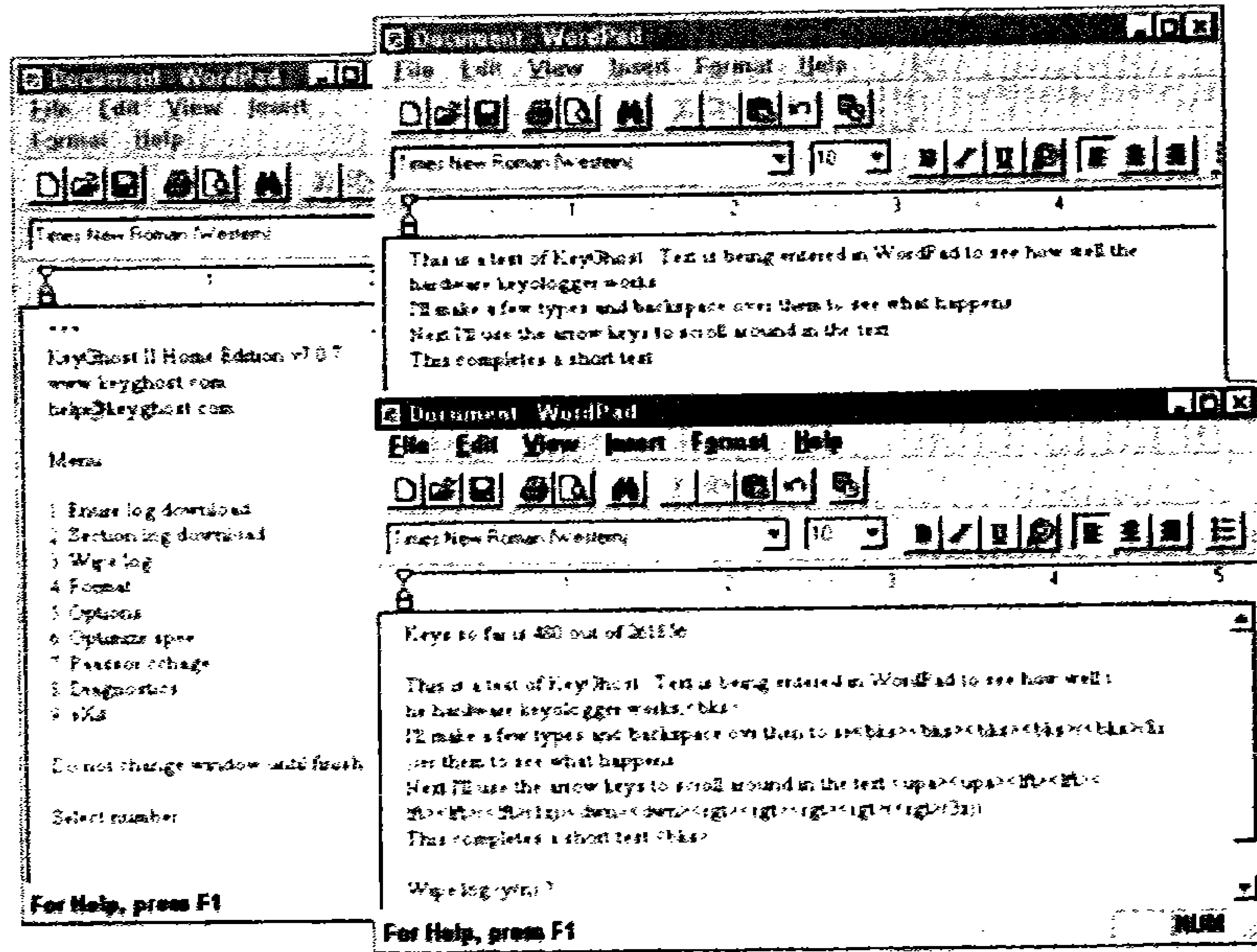
الشكل (8-1) مسجلات مفاتيح صلبة KeyKatcher و KeyGhost. إذا صادفت مثل هذه الأجهزة موصولة إلى حاسبك، فإنك مراقب.

من أجل إدارة مسجل المفاتيح، مع العلم أن الأسلاك الكهربائية تراقب ضربات المفاتيح بصورة مستمرة، حالما يدخل مستخدم مسجل المفاتيح كلمة المرور في نافذة إدخال النص لمعالج تحرير النصوص Word، يرسل مسجل المفاتيح الخرج إلى معالج النصوص والذي يعرض قائمة نصية. باختيارك خيارات محددة من هذه القائمة تستطيع استعراض المفاتيح المسجلة، تغيير كلمات المرور، وإنجاز وظائف إدارية أخرى (انظر الشكل 8-2).

لا داعي لأن تملك وصولاً فيزيائياً إلى الحاسب المركب عليه مسجل المفاتيح للحصول على ضربات المفاتيح. ما عليك إلا فك توصيل هذا الجهاز من الحاسب الهدف ووصله بحاسب آخر في مكان آمن لفحص النتائج.

ميزات ومساوئ مسجلات المفاتيح الصلبة

توجد حسنات ومساوئ لاستخدام مسجلات المفاتيح البرمجية والصلبة. عليك توخي الحذر من بعض نقاط القوة والضعف العامة لكلا النوعين قبل أن تقرر النوع الذي يناسبك.



الشكل (8-2) تمثل النافذة اليسرى قائمة مسجل المفاتيح KeyGhost عندما تكتب كلمة المرور الخاصة بمسجل المفاتيح في محرر نصوص. وتظهر النافذة العليا نصاً مدخلاً في برنامج الدفتر. وتظهر النافذة السفلى ماذا سجل KeyGhost، ومن بينها حركات الحذف والأسهم.

محاسن مسجلات المفاتيح الصلبة: تتميز مسجلات المفاتيح الصلبة بمجموعة من المحاسن مقارنة مع مسجلات المفاتيح البرمجية، ومن بينها ما يلي:

- لا يمكن كشف هذه الأجهزة من قبل برمجيات كشف مسجلات المفاتيح. حيث لا تعمل التقنيات القياسية وأدوات كشف مسجلات المفاتيح البرمجية لعدم وجود أية ملفات تم تثبيتها أو أية عمليات تم تشغيلها على مستوى نظام التشغيل، أو أية إشارة تدل على ملفات سجل.

- تتميز مسجلات المفاتيح الصلبة بإمكانية تثبيتها بسرعة وبسهولة فائقة. قم بتوصيل مسجل المفاتيح إلى منفذ لوحة المفاتيح في الحاسب، ومن ثم قم بتوصيل سلك لوحة المفاتيح إلى مسجل المفاتيح، ويصبح مسجل المفاتيح جاهزاً للعمل. ليس من الضروري تشغيل الحاسب من أجل تثبيت مسجل المفاتيح. وهذا أمر جيد جداً إذا قام مستخدم ذكي بحماية حاسبه بكلمة مرور صعبة التوقع سواء لعملية تسجيل الدخول أو لنظام الدخل والخرج الأساسي BIOS.
- مسجلات المفاتيح الصلبة مستقلة عن نوع نظام التشغيل لحواسب Intel. هذا يعني أن الجهاز سوف يعمل بصورة صحيحة مع نظام التشغيل DOS، Windows 95، Linux، Windows XP، أو أي نظام تشغيل آخر يعمل على الحاسب الشخصي. تقوم هذه الأجهزة بتسجيل المفاتيح المدخلة خلال بدء تشغيل برنامج النظام BIOS.
- لا تحتاج مسجلات المفاتيح الصلبة مصدراً مستقلاً للطاقة، حيث يقوم التيار القادم من منفذ لوحة المفاتيح بتغذيتها.

مساوئ مسجلات المفاتيح الصلبة: مع أن مسجلات المفاتيح الصلبة تبدو كأنها الجهاز المثالي للتنصت على لوحة المفاتيح، لكنها تعاني من بعض القيود.

- الحاجة إلى الوصول الفيزيائي للحاسب الهدف. وبالمقابل تقدم بعض مسجلات المفاتيح البرمجية إمكانية تثبيت مسجل المفاتيح عن بعد دون التعرض لخطر الكشف.
- يزيد سعر مسجلات المفاتيح الصلبة من ضعفين إلى ستة أضعاف بالمقارنة مع مسجلات المفاتيح البرمجية المشابهة. ومع ذلك تعتبر الأجهزة غير مكلفة نسبياً، مع وصول أعلى كلفة لمسجل مفاتيح تجاري إلى أقل من 300 دولار أمريكي.
- تلتقط هذه الأجهزة ضربات المفاتيح فقط، بينما مسجلات المفاتيح البرمجية يمكن أن تلتقط عرض الشاشة بالإضافة إلى حركة الفأرة، النقرات، ومعلومات أخرى.
- لا تتمتع مسجلات المفاتيح الصلبة بمقدار كبير من الخفية مقارنة مع مسجلات المفاتيح البرمجية، باستثناء مسجلات المفاتيح التي تركب في داخل لوحة المفاتيح. فقد يتساءل المستخدم الحاسبي الذكي عن الوصلة الزائدة المعلقة بلوحة المفاتيح في حاسبه، ومع أن هذا النوع من مسجلات المفاتيح مصمم ليبدو تماماً مثل الوصلة المعروفة أو المرشح الموازن المتضمن، إلا أنها مباشرة ستثير شكوك المستخدم الذي يعرف عما يبحث.
- لا تمتلك هذه الأجهزة طريقة لإرسال ضربات المفاتيح الناتجة آلياً لحاسب آخر عبر الشبكة. لتحقيق هذا عليك أن تبرمج أداة مخصصة للتفاعل مع مسجل المفاتيح للقيام سرياً بتحميل المعلومات وإرسالها إلى مكان آخر.

- لن تعمل مسجلات المفاتيح الصلبة على الحواسب المحمولة، وهذا يعتبر عائقاً كبيراً إذا كنت تتجسس على مدراء الأعمال المسافرين.
- حالياً، لا تعمل مسجلات المفاتيح الصلبة مع لوحات المفاتيح ذات المنفذ USB، بل تعمل مع لوحات المفاتيح ذات المنفذ PS/2 والطرز الأقدم من لوحات المفاتيح AT. من المحتمل تماماً أن الحكومة والجواسيس المُموّلون جيداً يملكون مسجلات المفاتيح للمنفذ USB، لكنها غير متوفرة في الوقت الحاضر للعامة. من المتوقع خلال السنوات القليلة القادمة،أن تصل إصدارات تجارية لمسجلات المفاتيح الصلبة إلى الأسواق.

أدوات مسجل المفاتيح

أما الآن وبعد أن تكونت لديك فكرة عامة عن مسجلات المفاتيح، سوف نستعرض بعض الأمثلة عن منتجات برمجية وصلبة يمكنك استخدامها للتجسس على الناس. حيث أن مسجلات المفاتيح استثمار غير مكلف ورخيص لأي شخص مهتم بالتجسس الحاسبي. قد تكون مهتماً بالحصول على عدة أنواع مختلفة منها لتقابل احتياجاتك الخاصة.

مسجلات المفاتيح البرمجية

هناك عدد كبير جداً من برمجيات مسجلات المفاتيح على شبكة الإنترنت، بحيث يتطلب شرحها جميعاً كتاباً كاملاً وسوف يكون مضجراً جداً على الأغلب إلا للجواسيس المحترفين كثيراً. نناقش من خلال هذه الفقرة بعض برامج مسجلات المفاتيح المعروفة والشعبية. كما يقدم بائعو مسجلات المفاتيح البرمجية الأكثر تطوراً وتعقيداً منتجات مراقبة متنوعة جداً، وتتراوح من منتجات ذات ميزات محدودة مناسبة للاستعمال المنزلي، إلى إصدارات احترافية ذات ميزات متقدمة مثل إرسال البيانات عن بعد. كما تحوي معظم الإصدارات التجارية نسخاً تجريبية يمكنك تحميلها وتقييمها لتتأكد من أنها ترضي جميع احتياجاتك (مع تطبيق بعض الإجراءات المضادة التي سوف نذكرها لاحقاً في هذا الفصل، لتعرف مدى صعوبة أن يكتشف هدفك محاولات التجسس التي تقوم بها).

Spector Professional Edition: وهو من أفضل منتجات شركة SpectorSoft (بعض الشيفرة المستخدمة في مسجلات المفاتيح لهذه الشركة مبنية على حصان طروادة Netbus). يسجل هذا البرنامج المفاتيح بالإضافة إلى البريد الإلكتروني، جلسات الدردشة، الرسائل الفورية، وشاشات العرض. كما أنتجت شركة SpectorSoft برنامجاً يدعى eBlaster يقوم، بالإضافة إلى تسجيل ضربات المفاتيح، بإرسال تقارير عبر البريد الإلكتروني حول نشاطات الهدف كل ثلاثين دقيقة.

وقد صرح بعض المستخدمين أنه يتم إعادة إرسال البيانات المشفرة إلى شركة SpectorSoft عندما يستخدمون مسجلات المفاتيح. صرحت الشركة أن هذا ضروري لنظام الإنذار الخاص ببريدها الإلكتروني، لكن قد يقلق جاسوس مرتاب من عملية إرسال البيانات إلى طرف ثالث. تبلغ كلفة كلا إصداري Spector Professional Edition و eBlaster قيمة 99 دولاراً أمريكياً، وتتوفر على الرابط www.spectorsoft.com.

Invisible Keylogger Stealth (IKS): كما هو واضح من اسم البرنامج، يعتبر مسجل المفاتيح IKS من أحد مسجلات المفاتيح التجارية الأكثر خفية، وهو مسجل مفاتيح لبرنامج تشغيل الجهاز Device Driver keylogger، مع توفر إصدارات مختلفة لأنظمة التشغيل Windows 9x/Me، NT، و 2000/XP. يقوم برنامج IKS بتجميع ضربات المفاتيح فقط، على خلاف بقية مسجلات المفاتيح التجارية والتي تتضمن كل ميزات المراقبة. تتوفر برامج خدمية أخرى لاستعراض ملف السجل وإرسال البيانات المسجلة سرياً عبر البريد الإلكتروني. كما يعتبر IKS من مسجلات المفاتيح القليلة التي تستطيع التقاط ضربات المفاتيح لمربع حوار تسجيل الدخول Ctrl+Alt+Del في أنظمة التشغيل Windows 2000/XP، كما أصدر المصّنع شيفرة مخصصة للبرنامج مصممة لخداع برامج كشف مسجلات المفاتيح والتي تقوم بعملية بحث عن حجم ملف محدد أو محرفاً ثنائياً لكشف IKS. يكلف إصدار البرنامج لأنظمة التشغيل Windows 2000/XP 99 دولار أمريكي ويمكن طلبها من الموقع www.amecisco.com.

وفيما يلي بعض المصادر لمراجعات معمقة ومستقلة لمسجلات المفاتيح:

- نشرت الجمعية الوطنية للإحصائيات والمعلومات القضائية (www.search.org)، في شهر تموز عام 2001، مراجعة لمسجلات المفاتيح التجارية المصممة لمساعدة الموظفين القضائيين المسؤولين عن مراقبة الموضوعين تحت الاختبار، على اختيار البرمجيات اللازمة لمراقبة النشاطات الحاسبية للأشخاص الخاضعين لإشرافهم لانتهاكات ارتكبوها أثناء فترة اختبارهم. لم يعد الإصدار بتنسيق PDF من هذا المستند متوفراً على موقع الويب التابع للمنظمة، لكن يمكنك الحصول على إصدار HTML وذلك لإجراء بحث على المحرك Google للنص: "Desktop Monitoring and Surveillance Software".
- أجرت مجلة PC Magazine مراجعة حول مسجلات المفاتيح التجارية في شهر تموز عام 2002، ويمكنك الإطلاع على النتائج من خلال الرابط:

www.pcmag.com/article2/0.4149.272723.00.asp.

WINWHATWHERE INVESTIGATOR: ظهر هذا المنتج منذ عام 1993، وقد كان مصمماً في بداية الأمر كأداة لإدارة المشاريع لتعقب استخدام البرمجيات. وفي عام 1998، تمت إعادة

تصميمه للاستفادة من الاهتمام المتزايد بالتنصت الحاسبي. يقوم برنامج Investigator، وهو مراقب كامل المواصفات، لتسجيل ضربات المفاتيح، شاشات العرض، كاميرات الويب، وتشغيل التطبيقات. ويتميز أيضاً بميزة ظريفة جداً وهي قدرته على إزالة نفسه من الحاسب الهدف بعد فترة زمنية محددة. النقطة السلبية الرئيسة في برنامج Investigator هي في حجمه الكبير (مبرمج بلغة Visual Basic)، وما لم تستطع إقناع مستخدم بأن يفتح ملفاً مرفقاً بحجم 3MB، فإنه لا يكون مناسباً للاستخدام البعيد. يتوفر البرنامج على الرابط www.winwhatwhere.com ويكلف 100 دولار أمريكي.

مسجلات المفاتيح الصلبة

على خلاف مئات الشركات المطورة لمسجلات المفاتيح البرمجية المتوفرة عبر شبكة الإنترنت، يوجد عدد محدود من الشركات التي تقوم بتصنيع مسجلات المفاتيح الصلبة التجارية. تتضمن المنتجات الصلبة ما يلي:

KEYGHOST: تعد شركة Interface Security النيوزيلاندية، من الرواد والمبتكرين في مجال مسجلات المفاتيح الصلبة. منتج الشركة KeyGhost يبدو مثل سلك له مرشح موازن داخلي. يوصل طرف من سلك لوحة المفاتيح إلى أحد أطراف مسجل المفاتيح، ويوصل الطرف الآخر إلى منفذ لوحة المفاتيح في الحاسب. بعد أن تقوم بوصل مسجل المفاتيح KeyGhost يبدأ بتسجيل ضربات المفاتيح. يتم تكوين الجهاز بعد طباعة كلمة المرور الصحيحة في أي محرر نصوص، بما أن المنتج KeyGhost يراقب ضربات المفاتيح، عندما تتم طباعة كلمة المرور الصحيحة، يقوم الجهاز بإرسال سلسلة ضربات المفاتيح إلى محرر النصوص نفسه والتي تستعرض قائمة الأوامر. تتضمن خيارات القائمة تحميل وإزالة ملف السجل الحالي، تغيير كلمة المرور، ونشاطات تكوين أخرى.

واجهة لوحة المفاتيح في الحاسب المكتبي غير مصممة للاتصالات عالية السرعة، وقد تستغرق عملية تحميل محتويات مسجل مفاتيح صلب فترة زمنية ليست قصيرة (حوالي 150 محرفاً في الثانية). وإذا كان مسجل المفاتيح يجمع البيانات لفترة من الزمن، سوف يستغرق تحميل ضربات المفاتيح بحجم نصف ميغا بايت حوالي ساعة من الزمن. يوجه المصنّع التحميلات البطيئة باستخدام منتج آخر يسمى Turbo Download Adaptor، حيث تقوم باستخدامه وصل أحد الأطراف إلى مسجل المفاتيح والطرف الآخر إلى منفذ تسلسلي في الحاسب. يدعم البرنامج باستخدام برنامج خاص تحميلا ت أسرع بكثير تصل إلى 56-Kbps لبيانات مسجل المفاتيح.

تكلّف منتجات KeyGhost من 89 دولاراً أمريكياً للإصدار Home Edition والذي يخزن 128K من البيانات إلى الإصدار Professional بقيمة 199 دولاراً أمريكياً والذي يخزن 2MB من البيانات ويقوم بتشفير البيانات التي يخزنها. كما تقدم الشركة لوحات مفاتيح مع مسجلات مفاتيح مدمجة بداخلها. تتوفر هذه المنتجات على الرابط www.keyghost.com.

KEYKATCHER: يفضّل مطور جهاز KeyKatcher أن يدعو منتجه "آلة تسجيل للوحة المفاتيح" ويختلف مسجل المفاتيح الصلب KeyKatcher في مظهره عن الجهازين KeyGhost وKeyLogger. حيث بدلاً من استخدام تكوين السلك، يملك الجهاز KeyKatcher أسلاكه الكهربائية مركبة داخلياً في وصلة صغيرة توصل بدورها إلى منفذ لوحة المفاتيح، ويوصل سلك لوحة المفاتيح إلى هذه الوصلة، ويأتي مع الجهاز قطعة من الأنابيب التي تتقلص بالحرارة والتي يمكنك أن توصلها إلى سلك ووصلة لوحة المفاتيح إذا أحببت. هذا يجعل المنتج أكثر خفية من المنتجات ذات الأسلاك المضمنة داخلياً.

يعمل الجهاز KeyKatcher تماماً مثل باقي مسجلات المفاتيح الصلبة، عند استخدام محرر نصوص وكلمة مرور للوصول إلى قائمة الأوامر. لكن يعاني الجهاز KeyKatcher من نقص في التغذية الكهربائية في قسم الذاكرة مقارنة مع مسجلات المفاتيح الصلبة الأخرى لأنه يخزن 64K من البيانات فقط كحد أعظمي (ذاكرة أقل تعني حجماً أقل). هذا المنتج مناسب لعمليات المراقبة القصيرة أو في الحالات التي لا يقوم المستخدم بإدخال الكثير من البيانات إلى الحاسب. الجهاز KeyKatcher فريد لأن كل قطعة منه تتضمن رقماً تسلسلياً مسجلاً من قبل المصنّع، وهذا أمر جيد لتعقب أثر الشخص الذي قام بشراء أحد هذه الأجهزة التي تم تركيبها بشكل سري.

يبلغ سعر الطراز الرئيسي للجهاز ذو 8K من الذاكرة 45 دولار أمريكي، تتوفر إصدارات ذات الذواكر 32K و64K بالأسعار 59 و 79 دولار أمريكي، ويمكنك زيارة موقع الشركة www.keykatcher.com.

HARDWARE KEYLOGGER: تصنّع شركة Amecisco منتجات مسجلات المفاتيح الصلبة إلى جانب منتجاتها البرمجية مثل البرنامج IKS. حيث الجهاز Hardware KeyLogger هو سلك يصل بين لوحة المفاتيح والحاسب وذلك لالتقاط ضربات المفاتيح مثل الجهاز KeyGhost. يتم تخزين ضربات المفاتيح في ذاكرة دائمة، حجمها يتراوح بين 512K و 2MB، بحسب الطراز، وتعرض قائمة بالأوامر عندما يتم إدخال كلمة المرور الصحيحة ضمن أي محرر نصوص.

هناك منتج آخر لشركة Amecisco أكثر مكراً من سابقه، وهو إصدار للوحة المفاتيح مع الجهاز Hardware KeyLogger. حيث يشتري البائع لوحات المفاتيح مباشرة من المصنّع ويقوم بتركيب رقاقة التسجيل داخل لوحة المفاتيح. يمكنك طلب الإصدار المراقب لأنواع مختلفة من لوحات

المفاتيح. حيث أن استبدال لوحات المفاتيح ينجح مع الحواسب الجديدة، لكنه يصبح أصعب عند استبدال لوحة مفاتيح أقدم والتي قد تحوي تراكماً للأوساخ وبقع من الطعام. لذلك تقدم الشركة لوحات مفاتيح مستعملة من الصعب كشفها، بناءً على طلب الزبائن.

تسعّر منتجات مسجلات المفاتيح من 99 دولاراً أمريكياً للإصدار الذي يخزن 512K من البيانات إلى 199 دولاراً أمريكياً للإصدار الذي يخزن 2MB من البيانات. أما قيمة نماذج لوحة المفاتيح تتراوح من 129 إلى 299 دولاراً أمريكياً. وتتوفر معلومات كاملة حول هذه المنتجات على موقع الشركة www.amecisco.com.

مضبوط: مع كل الحب من روسيا

استخدمت حكومة الولايات المتحدة، خلال عملية الاحتيال "شركة Invita" التي قام بها مكتب التحقيقات الفدرالي (مرت معنا في الفصل الأول) والتي انتهت باعتقال مخربين من روسيا، مسجل مفاتيح تجاري WinWhatWhere Investigator للحصول على الأدلة المطلوبة. وقد انتشرت محتويات الشهادة الخطية المتعلقة بالقضية الصادرة عن العميل الخاص Michael Schuler، مع أنه طالب أن تبقى محتوياتها مختومة. وفيما يلي نظرة ممتعة على هذه العملية.

قام عملاء مكتب التحقيقات الفدرالي بتثبيت مسجل المعاتيح WinWhatWhere على حاسبين، ثم استخدم أحد المشتبهين Gorshkov الحاسب المراقب (من طراز IBM) للاتصال بالحاسب البعيد freebsd.tech.net.ru باستخدام البروتوكول Telnet عبر شبكة الإنترنت. لكن Gorshkov لم يكن يعلم أن حسابه "kvakin" وكلمة المرور "cfvlevfq" قد التقطا من قبل مسجل المفاتيح. حاول Schuler، بعد اعتقال Gorshkov، أن يتصل بالحاسب البعيد freebsd لكن جميع محاولاته باءت بالفشل (يبدو أنه قد استخدم الاسم بدلاً من استخدام عنوان IP). ثم دخل إلى الموقع www.samspade.org واستخدم خدمة "من هو" أو "whois"[1] لتحديد أن الحاسب freebsd كان جزءاً من شبكة متصلة بالملقم tech.net.ru، وأخيراً تمكن Schuler من تسجيل الدخول إلى الشبكة tech.net.ru باستخدام البروتوكول Telnet، ومن ثم استخدم خدمة cuteFTP محاولاً تحميل محتويات الحاسب.

ثم جلب العميل Schuler خبيراً أمنياً مدنياً (لا يعمل لصالح قوى القانون) ليساعده في تحميل الملفات. (يبدو من الشهادة أنه كان فوق طاقة العميل Schuler التعامل مع حواسب Unix). تحقق الخبير الأمني من كمية المساحة المستخدمة القرص على كل حاسب ومن ثم ضغط المحتويات باستخدام خدمة tar ومن ثم قام بتحميلها ثانية باستخدام البروتوكول FTP إلى مقر مكتب التحقيقات الفدرالي في Seattle .

[1] خدمة "من هو whois": خدمة في شبكة الإنترنت تمكن المستخدم من إيجاد عناوين المستخدمين الآخرين وبعض المعلومات الأخرى الموجودة في قوائم بيانات خاصة.

ملاحظة إلى الجواسيس الناشئين: لا تثق أبداً بحاسب أو شبكة شخص آخر قبل أن تستعرض مهاراتك للعمل، أو قد يتم خداعك مثل ما حصل للروسيين حيث اعتقدا أنهم سيتلقيان وظيفة ذات رواتب عالية.

التجهيزات المخصصة: تعمل مسجلات المفاتيح التجارية بصورة ممتازة، وخاصة الإصدارات الخفية من لوحة المفاتيح، لكن قد تكون هناك حالات عندما تواجه هدفاً صعباً وتحتاج إلى مسجل مفاتيح يتحدى فعلياً الكشف. إذا كانت الموارد الحكومية أو المدمجة متوفرة تحت تصرفك، فقد يكون من المناسب استخدام تجهيزات مصممة بشكل مخصص لتستخدم ضد هدف خبير تقنياً. يمكن تطوير مسجل مفاتيح مخصص ليتسع داخل لوحة المفاتيح، صندوق الحاسب الشخصي، أو الحاسب المحمول وليكون حجمه صغيراً ليتوارى عن الأنظار لتجنب كشفه. كذلك من الممكن أيضاً استخدام مسجل مفاتيح صلب بالتوافق مع التجهيزات الشبكية المصممة خصيصاً لتمرير المعلومات الناتجة عبر اتصال شبكي. بالطبع ستكون تكلفة مثل هذا الجهاز عالية، لكنها ستكون أيضاً فعالة جداً في عملية تجسس عالية المستوى.

وسائل التجارة: الفانوس السحري لمكتب التحقيقات الفدرالي

بدأت تنتشر معلومات حول مشروع تابع لمكتب التحقيقات الفدرالي سمي بالفانوس السحري "Magic Lantern"، عام 2001، والذي تم وصفه بأنه مسجل مفاتيح خاص بقوى القانون والذي يمكن أن يتم تثبيته عن بعد على الحاسب إذا فتح المستخدم رسالة إلكترونية تتضمن تطبيق حصان طروادة. ولسوء الحظ حصلت وسائل الإعلان على بعض الوقائع الخاطئة حول هذا المشروع ووصفت البرنامج على أنه فيروس، ثم بدأت الأمور تخرج عن السيطرة. حيث اتصل المسؤولون عن الشبكة بمكتب التحقيقات الفدرالي فرضياً، وأكدوا أن برنامج مكافحة الفيروسات McAfee لن يقوم بكشف الفانوس السحري لكي لا تنقطع التحقيقات. (زعم بائعو برمجيات مكافحة الفيروسات Symantec و Sophos أنهم لن يعيروا أي اهتمام للفانوس السحري وسيقومون بكشفه وحذفه مثل أي برنامج خبيث آخر). سبب هذا الأمر انتهاكاً مع المدافعين عن حقوق الخصوصية الإلكترونية، ونكر المسؤولون عن الشبكة تورطهم بأي تصريح يتعلق بالفانوس السحري. كما أظهر بعض المحللين الأمنيين الإصدار الصحفي الذي جعل المسؤولين عن الشبكة يتدخلون بمشاريع مماثلة مع الحكومة وليس بالضرورة مشروع الفانوس السحري. ومن ثم تدخل الباحثون النظريون في المؤامرة في هذه الفعالية الرائجة، معتبرين أن المسؤولون عن الشبكة يقومون بمنح قوى القانون أبواباً ملتوية لاختراق التطبيق PGP، حيث تم بيع في هذه الفترة منتجات التشفير التجارية للتطبيق PGP.

لم تخل هذه القصة المتعلقة بالفانوس السحري من بعض المواقف الطريفة. حيث سخر أحد المشاركين في نقاش على الشبكة من برنامج المراقبة هذا قائلاً، "هذا البرنامج سوف يعمل بشروط أ) يقتحم مكتب التحقيقات الفدرالي منزلك وينصبون برنامج Outlook، ب) تقوم دائماً بفتح رسالة إلكترونية بعنوان 'الأميرة النائمة وعملاء FBI السبعة'، ج) تقوم بتشغيل الملف المرفق FBILOVESYOU.VBS."

ظهرت الكثير من الشائعات حول مشروع الفانوس السحري، لكن لم تظهر أية تفاصيل دقيقة حول الموضوع. اعترف مكتب التحقيقات الفدرالي أن الفانوس السحري كان "مشروع عمل"، وجزءاً من مجموعة من أدوات برمجية للتحقيقات الفدرالية الملقبة "الفارس الإلكتروني."

الإجراءات المضادة

أفضل إجراء مضاد ضد جاسوس يستخدم مسجل المفاتيح هو الأمن الفيزيائي. حيث تقلص حماية الحاسب من الوصول الفيزيائي فرص تركيب مسجل مفاتيح بشكل سري على حاسبك. (لكن لا يزال هناك خطر تثبيت مسجل مفاتيح عن بعد على حاسبك، لكنك إذا اتبعت إرشادات السلامة عند التعامل مع الملفات المرفقة وتدربت على أمن الشبكة العام، سيخفف هذا الخطر بشكل كبير).



ارجع إلى الفصل الثالث، لمزيد من المعلومات حول الأمن الفيزيائي.

بالرغم من كل المكر والخداع المرتبط بمسجلات المفاتيح، إلا أنها تترك نموذجياً بعض الآثار ورائها. ويمكنك تطبيق عدداً من الإجراءات المضادة لاكتشاف والتغلب على أنواع مختلفة من مسجلات المفاتيح.

استعراض البرامج التي تم تثبيتها

من لوحة التحكم افتح خدمة إضافة/ إزالة برامج لاستعراض جميع البرامج التي تم تثبيتها على الحاسب باستخدام برنامج مثبت. ابحث عن البرامج التي لم تقم بتثبيتها أو لا تعرف الغرض منها، لا تتفاجأ كثيراً، حيث يكشف هذا الإجراء البسيط بعض مسجلات المفاتيح التجارية.

تفحص برامج بدء التشغيل

من الجلي أنه ليعمل مسجلّ المفاتيح يجب أن يتم تشغيله أولاً. كما تضع برامج تثبيت مسجلات المفاتيح تعليمات ليتم تشغيل التسجيل في أحد الأماكن التالية:

- ملف Autoexec.bat
- مجلد بدء التشغيل Startup
- تسجيل النظام Registry

تستخدم مسجلات المفاتيح معظم الأحيان تسجيل النظام لإخفاء معلومات وتعليمات التشغيل للبرنامج لأن معظم المستخدمين لا يبحثون ضمن تسجيل النظام. للتحقق من برامج بدء التشغيل في التسجيل، استخدم الأداة RegEdit وابحث عن القيم الغريبة المدخلة ضمن المفاتيح التالية:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

عليك إقلاع الحاسب بالوضع الآمن Safe Mode قبل تفحص قيم تسجيل النظام. حيث تعدل بعض مسجلات المفاتيح قيم مفاتيح التشغيل بعد أن يتم تحميلها لكي لا يتم كشفها باستخدام الأداة RegEdit. أما في الوضع الآمن فلن يتم تحميل مسجل المفاتيح وسوف يتم إظهار قيم التسجيل التي تحدد مسار ملف مسجل المفاتيح.

تتضمن أنظمة التشغيل Windows 9x/ME خدمة تكوين النظام المسماة MSCONFIG.EXE، حيث يدعك البرنامج تفحص محتويات الملفات AUTOEXEC.BAT، Win.ini، وبرامج بدء التشغيل. تفيد هذه الأداة في اكتشاف مسجلات المفاتيح التي أعدت لتعمل تلقائياً عند بدء تشغيل النظام Windows.

إجراءات مضادة: تزييف المعلومات

ماذا يجب أن تفعل إذا وجدت مسجل مفاتيح مثبت على حاسبك؟ مع أنك سوف تحاول فوراً أن تلغي تثبيته، قد تفكر استخدامه كجزء من حملة تزييف معلومات ضد الجاسوس الذي قام بتثبيته. إذا رجعنا إلى الأسئلة الأساسية التي ناقشناها في الفصل الأول، من تعتقد الجاسوس، وما هو مسعاه؟ عليك أن تبحث قليلاً لمعرفة ما هو نوع مسجل المفاتيح الذي يعمل على حاسبك، وإذا وجدت ملف السجل تحقق من تاريخ إنشائه لتعرف المدة الزمنية التي ظل مسجل المفاتيح يجمع المعلومات عنك (تذكّر أن التاريخ يمكن أن يكون مزيفاً أيضاً). بعد أن تقوم بتقدير الفترة التي تواجد فيها مسجل المفاتيح على حاسبك، حاول الوصول إلى كمية الضرر الذي وقع أثناء عمله. ما هي الأعمال التي كنت تقوم بها؟ مع من كنت تجري اتصالاتك؟ كم مرة قمت بتصفح الإنترنت أو استخدمت برمجيات تتطلب كلمة مرور؟

إذا حاولت تمرير معلومات مزيفة إلى الجاسوس، سوف تحتاج إلى استخدام حاسب آمن لتقوم بأعمالك اليومية، واستخدم حاسبك المراقب فقط عند تنفيذ استراتيجية الخداع التي تخطط لها، يمكنك بدلاً من ذلك استخدام حاسبك الأصلي مع توخي الحذر لكي لا تكشف أية معلومات حساسة.

ما هو نوع المعلومات الذي يجب أن تدخله في حملة التزييف؟ المستندات والاتصالات التي قد تغطي نشاطاتك الحقيقية، المعلومات التي سوف تعارض الأمور التي قد تم كشفها من قبل مسجل المفاتيح، أو ذكر أسماء الأشخاص المحتملين المتورطين في عملية التجسس، أي سوف تجعل الخصم يعتقد أن الأشخاص الموثوقين على جانبه، فعلياً هم يعملون لصالحك. مثلاً، إذا راودتك الشكوك أنه تم كشف معلومات حول عملية دمج شركات قريبة، يمكنك بسهولة إنشاء مجموعة من المستندات والرسائل الإلكترونية المزيفة والتي توضح أن عملية الدمج قد أخفقت، وتسعى شركتك حالياً إلى اكتساب منافس آخر.

لكن إذا كان خصمك معقداً، قد يشك في عملية التزييف لذلك عليك التخطيط لهذه العملية بشكل دقيق جداً. وتعتمد مدة عملية التزييف على أهدافك وكمية الجهد الذي ترغب أن تبذله عليها.

وإذا راودتك شكوك أن أحدهم قد استطاع الوصول إلى حاسبك، يمكنك تركيب وسائل مراقبة لتعرف الشخص الذي زرع مسجل المفاتيح. يمكنك فعل ذلك باستخدام أدوات متعددة تتراوح من تثبيت كاميرة مراقبة مكلفة إلى كاميرة ويب رخيصة وبرنامج لكشف الحركة.

تفحص العمليات التي تعمل حالياً

بعد معرفة وجود الملفات المجهولة أو غير العادية التي تعمل عند بدء تشغيل النظام Windows، تتلخص الخطوة التالية في تحديد إذا كان هناك أي عملية قد تكون مسجل مفاتيح.

مدير المهام TASK MANAGER

يمكننا وبسرعة عن طريق خدمة مدير المهام معرفة العمليات التي تعمل حالياً في النظام Windows. تستطيع تشغيل نافذة مدير المهام بإتباع ما يلي:

- لأنظمة التشغيل Windows3.x/9x/ME، اضغط المفاتيح Ctrl+Alt+Del.
- لأنظمة التشغيل Windows NT/2000/XP، اضغط بزر الفأرة اليمين على أي نقطة فارغة على شريط المهام ثم اختار مدير المهام (تستطيع أيضاً ضغط المفاتيح Ctrl+Alt+Del ومن ثم اختيار زر مدير المهام من مربع الحوار).

يزود مدير المهام القليل من المعلومات في أنظمة التشغيل Windows 9x/ME، بالإضافة إلى ذلك لن يظهر مسجل المفاتيح الخفي في نافذة مدير المهام في الإصدارات الأقدم من نظام Windows، لكن هذا غير صحيح في الأنظمة Windows NT/2000/XP، إلا عندما يكون مسجل المفاتيح مثبتاً مثل برنامج تشغيل.

مستكشف العمليات PROCESS EXPLORER

البديل الأفضل لمدير المهام، وهو خدمة مجانية من شركة Sysinternals ويسمى مستكشف العمليات Process Explorer. يعمل برنامج مستكشف العمليات على جميع إصدارات النظام Windows الأحدث من Windows 95، ويزود معلومات أكثر بكثير من مدير المهام. ويمثل مستكشف العمليات أداة كشف قيمة لاكتشاف مسجلات المفاتيح لأنه يعرض الملف الذي يقوم بتشغيل العملية، يمكنك تحميل مستكشف العمليات من الرابط www.sysinternals.com.

عندما تقوم بفحص العمليات قد تصادف أسماء عمليات غير معروفة، لكن لا تعتقد مباشرة أن العملية المجهولة هي مسجل المفاتيح، على الأرجح قد تكون برنامجاً أو خدمة عادية، لكن عليك قضاء وقتاً إضافياً للتأكد من العملية.

توجد طريقتان لتحديد العمليات الغريبة بشكل صحيح:

- أدخل اسم العملية أو الملف الذي ترتبط به في محرك البحث Google، ليبحث ضمن مواقع الويب والمجموعات الإخبارية عن وجود أي نظير، يعيد محرك البحث عادة معلومات حول العملية.
- يمكنك استشارة موقع ويب يحوي مراجع للعمليات، مثل:

www.answerthatwork.com/Tasklist_pages/tasklist.htm. تتضمن مثل هذه المواقع لوائح حديثة للعمليات، لأنظمة التشغيل Windows وغيرها، والتي تظهر غالباً في لوائح المهام.

MSINFO32

وهو برنامج خدمي آخر لاكتشاف مسجلات المفاتيح والبرامج المخفية الأخرى، يزودك هذا البرنامج بمعلومات متنوعة عن برمجيات وتجهيزات النظام مع برامج التشغيل التي تم تحميلها، والمهام التي تعمل، وبرامج بدء التشغيل التي تم تشغيلها (انظر الشكل 3-8). وهي أداة كشف فعالة جداً اتبع الخطوات التالية لاستخدام MSinfo32:

1. من قائمة ابدأ، اضغط زر تشغيل Run.
2. أدخل msinfo32
3. اضغط زر OK.

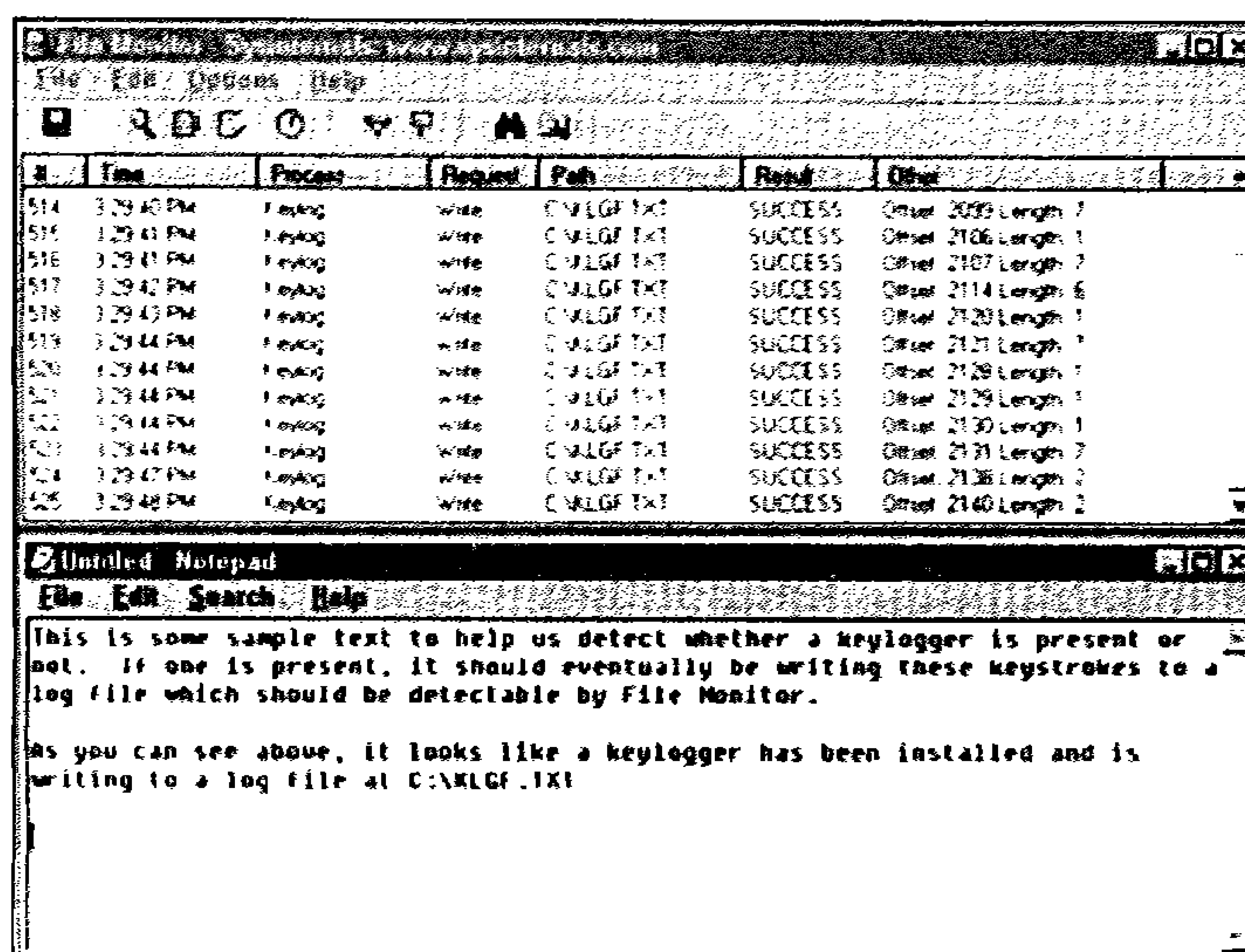
قد تجد معلومات تشير إلى مسجل مفاتيح مثبت ضمن مجلد Software Environment.

الشكل (3-8) لا يظهر برنامج keylog.exe في نافذة مدير المهام للنظام Windows 98. لكنه يظهر كعملية ضمن البرنامج الخدمي MSinfo32.

مراقبة نشاط الملفات

تخزن جميع مسجلات المفاتيح افتراضياً مجموعة من ضربات المفاتيح في ملف، وهذه إشارة هامة جداً لاكتشاف فيما إذا تم تثبيت مسجل المفاتيح على الحاسب. وعن طريق مراقبة الملفات التي تم تعديلها أو الكتابة عليها، تستطيع اكتشاف إذا كان مسجل المفاتيح فعال.

تزود عملية مراقبة الملفات File Monitor والتي تسمى غالباً Filemon مراقبة النظام في الزمن الحقيقي لنشاطات الملفات. حيث يعرض برنامج Filemon، عند الوصول إلى الملف أو فتحه أو إغلاقه، استرجاع سماته، قراءته أو الكتابة فوقه، التاريخ والوقت، العملية التي أجرت التغييرات، نوع طلب الملف الذي تم، ومسار الملف. تعتبر Filemon أداة فعالة جداً لتحديد مسجلات المفاتيح، وبالتالي يمكنك استعراض العملية المسؤولة عن كتابة البيانات إلى الملف إلى جانب اسم الملف الذي يخزن ضربات المفاتيح (انظر الشكل 8-4).



الشكل (8-4) برنامج Filemon وهو يكشف عملية الكتابة إلى ملف مسجل المفاتيح عند إدخال النص في المفكرة.

تستطيع استخدام هذا البرنامج الخدمي المجاني عن طريق تحميله من الموقع www.sysinternals.com وإتباع تعليمات التثبيت. (إذا كنت تعمل على أحد أنظمة التشغيل Windows NT/2000/XP، عليك تسجيل الدخول إلى حساب المدير لتعمل الأداة بصورة صحيحة). اتبع الخطوات التالية:

1. إغلاق جميع البرامج التي تعمل حالياً.
2. تنفيذ Filemon.
3. اختيار أيقونة Filter من شريط الأدوات (أو اضغط Ctrl + L).
4. تحديد مربع الاختيار Log Writes. ويحدد هذا الخيار البيانات المعروضة إلى تعديلات الملفات فقط.

5. ضغط زر تطبيق Apply.

6. اختيار أيقونة الالتقاط Capture (العدسة المكبرة) من شريط الأدوات، (أو اختيار الخيار التقاط Capture من قائمة خيارات Options أو اضغط Ctrl+E).

بعد أن يبدأ برنامج Filemon باستعراض نشاط الملفات، افتح برنامج المفكرة أو الدفتر وابدأ بالطباعة. سوف تقوم مسجلات المفاتيح البرمجية بتخزين ضربات المفاتيح ضمن ذاكرة مؤقتة قبل أن تبدأ بتسجيلها في ملف السجل. لذلك وبحسب حجم الذاكرة المؤقتة عليك طباعة كمية نص مناسبة لجعل مسجل المفاتيح يكتب إلى الملف.

إذا لاحظت سلسلة من التعديلات المرتبطة بملف محدد، وليس هناك أي نشاط يقوم له النظام أو البرنامج، فقد تكون اكتشفت ملف السجل الخاص بمسجل المفاتيح.

إزالة أزمنة التنفيذ للغة البرمجة Visual Basic

هناك عدد من مسجلات المفاتيح المجانية والتجارية المطورة باستخدام لغة البرمجة Visual Basic وتعتمد على ملفات VB لزمن التنفيذ. وسوف يؤدي إزالة هذه الملفات، في حال لم تنفذ أي برامج تعتمد عليها، إلى إيقاف تنفيذ مسجلات المفاتيح المطورة بلغة البرمجة Visual Basic. وأسماء هذه الملفات، بحسب إصدار Visual Basic المستخدم، هي vbrun100.exe، vbrun200.exe، vbrun300.exe، vb4run.exe، MSVBM50.EXE، و vbrun60sp5.exe. ابحث ضمن القرص الصلب لديك عن وجود أي من هذه الملفات، ويمكنك ببساطة إعادة تسمية ملف زمن التنفيذ ومن ثم إعادة إقلاع الجهاز، لتمنع برنامج VB من استخدام ملف زمن التنفيذ. من الجلي أن هذه الطريقة لا توقف مسجلات المفاتيح المطورة باستخدام لغات برمجة أخرى.

البحث عن المحارف

اطبع سلسلة نصية فريدة، ضمن أي محرر نصوص، ثم انسخ جزءاً من السلسلة المحرفية واستخدم أمر ابحث Find (في أنظمة التشغيل Windows 9x/ME) أو الأمر بحث Search (في أنظمة التشغيل Windows 2000/XP) من قائمة ابدأ لتحديد موقع الملف الذي يتضمن هذه السلسلة المحرفية. تنجح هذه الطريقة مع مسجلات المفاتيح التي لا تقوم بتشفير محتويات ملف السجل.

استخدام جدار حماية شخصي Personal Firewall

من المحتمل ألا يقوم مسجل المفاتيح بأي تعديلات على القرص إنما يرسل المعلومات مباشرة عبر الإنترنت، ضمن حاسب متصل بشبكة. في هذه الحالة لن يكشف البرنامج Filemon ملف السجل لأنه لم يتم إرسال إي طلبات للملف.

إن تثبيت جدار حماية (مثل ZoneAlarm، والذي يؤكد إمكانية السماح لوقوع اتصالات شبكية من البرامج) سوف يتغلب على مسجل المفاتيح.

إذا تمكن الجاسوس من الوصول فيزيائياً إلى حاسبك، فقد يكون قد غير إعدادات جدار الحماية لمنح السماحيات إلى مسجل المفاتيح ليتمكن من الاتصال بشبكة الإنترنت. لذلك من الجدير التحقق دورياً من إعدادات جدار الحماية لضمان عدم وجود أي برامج مجهولة تتصل بالإنترنت دون إذن منك.

استخدام برامج تكامل الملفات ومدققات التسجيل

عندما يقوم الجاسوس بتثبيت مسجل مفاتيح برمجي، فمن الجلي أنه يجب أن يترك أثراً للبرنامج. لذلك قد يمنحك استخدام برنامج لتدقيق تكامل الملفات للبحث عن الملفات الجديدة المضافة إلى الدليل أو مراقب تسجيل النظام لتعقب آثار الإضافات والتعديلات الحديثة، علامات هامة حول تثبيت مسجل مفاتيح سرياً على حاسبك.

أساليب: التغلب على جدار الحماية

إحدى نقاط الضعف الكامنة التي يعاني منها جدار الحماية الشخصي هي أنه إذا تم استخدام تطبيق موثوق لإرسال المعلومات سرياً عبر شبكة الإنترنت. على سبيل المثال، يثق معظم المستخدمون بمستعرض الإنترنت Internet Explorer عند اتصاله بالإنترنت، لكن إذا استطاع أحد ما استغلال مستعرض الإنترنت ليقوم بإرسال المعلومات سرياً عبر الشبكة إلى موقع الجاسوس، فإن معظم برامج جدار الحماية الشخصية لن تستطيع كشفه.

طور Jason، وهو عضو في فريق تشفير ألماني، مسجل مفاتيح اسمه God يستفيد من نقطة الضعف هذه. حيث يقوم الجاسوس بوضع برنامج نصي php. على ملقم ويب ومن ثم يثبت مسجل المفاتيح God على الحاسب الهدف. وعندما يجمع مسجل المفاتيح البيانات يقوم بإرسال ضربات المفاتيح إلى ملقم الويب الذي ينفذ البرنامج النصي php. من خلال مستعرض الإنترنت Internet Explorer.

تتجاوز ضربات المفاتيح المسجلة الكشف، لأن معظم المستخدمين يحددون جدار الحماية لديهم بالسماح لمستعرض الإنترنت الاتصال دون طلب الإذن لذلك.

لمزيد من المعلومات عن مسجل المفاتيح God اتبع الرابط www.ratct.net، لكن تدرب على الألمانية لأن المقالة ليست باللغة الإنكليزية.



للحصول على تفاصيل كاملة عن مدققات تكامل الملفات ومراقبات التسجيل، راجع فقرة "الإجراءات المضادة" في الفصل التاسع.

استخدام برمجيات كشف مسجلات المفاتيح

يمكنك بدلاً من التحقق يدوياً عن وجود مسجلات مفاتيح مثبتة سرياً على حاسبك باستخدام بعض الخطوات أعلاه، استخدام عدد من المنتجات المنتشرة في الأسواق والتي تقوم بكشف وجود مسجل المفاتيح على حاسبك. ويوجد عدد من الإنذارات لاستخدام برمجيات كشف مسجلات المفاتيح بدلاً من مراقبة العمليات، نشاط الملفات، كما يلي:

- تعمل برمجيات الكشف على مسجلات المفاتيح المعروفة التي دونها البائع، حيث لا يتم كشف مسجلات المفاتيح الجديدة أو المجهولة.
- يمكن تشبيه هذه البرمجيات ببرنامج مكافحة الفيروسات. حيث يقدم البائع ملفات تعريف حديثة لمسجلات المفاتيح، فإذا استخدمت أحد هذه الأدوات يجب أن تقوم بتحديثها دورياً.
- قد تولد برمجيات الكشف "تنبيهاً زائفاً" (حيث تتم الإشارة إلى وجود مسجل مفاتيح، لكن فعلياً لا يوجد مسجل مفاتيح). فإذا صرح البرنامج عن وجود مسجل مفاتيح بناء على وجود ملف ذو اسم خاص، ابحث على شبكة الويب لمعرفة إذا كان ذلك الملف ينتمي إلى تطبيق آخر قمت بتثبيته وليس مسجل مفاتيح.

نعرض فيما يلي بعض البرامج الشائعة لكشف مسجلات المفاتيح.

SPYCOP

يزعم برنامج SpyCop بأنه قادر على كشف أكثر من 300 مسجل مفاتيح. عندما يكشف البرنامج SpyCop مسجل مفاتيح، يقدم للمستخدم خياراً لإعادة تسمية الملفات المرتبطة بالامتداد spy. (يمنع هذا الإجراء عادة من تشغيل مسجل المفاتيح، لكنه قد يسبب مشاكل أخرى). كما يقوم هذا البرنامج إلى جانب فحص جميع الملفات بحثاً عن وجود مسجلات

المفاتيح، بتوفير ميزة تفحص العمليات الجارية للتأكد من عدم وجود أي مسجلات مفاتيح. يمكنك تحميل نسخة تجريبية لبرنامج SpyCop وهي نسخة مختصرة ولا تفحص الملفات العشوائية، أما النسخة الكاملة للبرنامج فهي مسعرة بقيمة 69.95 دولار أمريكي وتتوفر على الرابط www.spycop.com.

WHO'S WATCHING ME

وهو كاشف آخر لمسجلات المفاتيح. يمكن إعداده ليعمل عند بدء التشغيل أو في أية لحظة أثناء عمل الحاسب. كما يقدم البرنامج تقريراً عن وجود مسجل مفاتيح ومعلومات حوله، لكنه لا يزيل مسجل المفاتيح من الحاسب. تتوفر نسخة تجريبية لهذا البرنامج لمدة تسعين يوماً (وهو مسعر بقيمة 24.95 دولار أمريكي) ويتوفر على الرابط www.trapware.com.

PEST PATROL

برنامج كامل الوظائف لكشف مسجلات المفاتيح وإزالتها، إلى جانب كشف تطبيقات حصان طروادة Trojan Horses، برامج الدودة worms، وبرامج التجسس المنتشرة. يفحص برنامج Pest Patrol جميع الملفات والعمليات الجارية ويزود معلومات مفصلة حول برامج التجسس التي قام بكشفها. تبلغ تكلفة البرنامج 29.95 دولار أمريكي، كما تتوفر نسخة تجريبية ذات وظائف محدودة على الرابط www.pestpatrol.com.

إجراءات مضادة: التنافس بين مسجلات المفاتيح وبرمجيات الكشف

صرحت القناة التلفزيونية MSNBC، في شهر آذار (مارس) عام 2002، عن قيام الشركات التجارية المطورة لمسجلات المفاتيح WinWhatWhere و SpectorSoft بإدراج شيفرة ضمن منتجاتها لتعطيل البرنامج المضاد المتداول Who's Watching Me.

حيث تم اقتباس تصريح لرئيس شركة WinWhatWhere قائلاً، "إذا حاول أحدهم كسب الأموال محاولاً تدمير برنامجي، سوف أضطر أن أتخذ موقفاً صارماً."

رد Wes Austin مطور برنامج Who's Watching Me، "كل ما نفعله هو إطلاع الناس عن وجود برنامج مراقبة. لذا ما هو سبب تدمير برنامج Who's Watching Me ما لم تكن تستخدم المنتج بصفة غير شرعية ومحاولاً إخفاء شيء ما... فهم يعلمون لماذا يستخدمه الناس."

لقد بدا الأمر وكأنه حرب برمجية محتمة واحدة بواحدة، مع حصول البائعين على إجراءات برمجية ليستخدموها ضد منتجات بعضهم. لكن الأمور هدأت بعد أن وصلت إلى الصحافة. وأعلنت

الشركة المالكة لبرنامج WinWhatWhere أنها لن تقوم بتعديل ملفات برنامج Who's Watching Me التي قامت بتعطيل خدمة كشف مسجلات المفاتيح.

SPYBOT SEARCH & DESTROY

أداة مجانية شائعة برمجها Patrick Kolla تكشف وتزيل مسجلات المفاتيح، تطبيقات حصان طروادة، برمجيات التجسس المنتشرة، والشيفرة الخبيثة الأخرى. يتمتع برنامج Kolla بعدد كبير من الميزات، ومن ضمنها التحديث عبر الإنترنت، إزالة آثار استخدام البرنامج، وواجهة متعددة اللغات. يتوفر برنامج SpyBot على الويب من خلال الرابط http://beam.to/spybotsd.

استخدام برامج الكشف Sniffers[1]

إذا راودك الشك أن مسجل المفاتيح يقوم بإرسال المعلومات سرياً إلى جاسوس، قم باستخدام برنامج كشف الحزمة packet sniffer مثل Ethereal لمراقبة حركة المرور على الشبكة. انتبه إلى بروتوكولات البريد الإلكتروني وتذكر أنه من الممكن أن يتم تشفير البيانات وبالتالي لن تستطيع قراءة محتواها. (لكن معظم مسجلات المفاتيح تستخدم تشفيراً ضعيفاً، أي يمكنك على الأرجح اختراق التشفير في فترة زمنية معقولة إذا كنت ماهراً قليلاً بأمور التشفير).



لمزيد من المعلومات عن برامج الكشف sniffers، انتقل إلى الفصل العاشر.

كشف مسجلات المفاتيح الصلبة

لا تستطيع جميع الأدوات والبرمجيات والتقنيات التي تكشف مسجلات المفاتيح البرمجية، والتي ناقشناها في الفقرات السابقة، أن تكشف مسجلات المفاتيح الصلبة. حيث يمكن كشف أجهزة المراقبة الصلبة، اعتماداً على نوعها، بسهولة كبيرة أو بصعوبة شديدة.

مسجلات المفاتيح المضمنة

كشف هذا النوع من مسجلات المفاتيح الصلبة سهل جداً. ابحث عن شيء غير عادي موصل إلى منفذ لوحة المفاتيح في الحاسب. تعقب السلك من لوحة المفاتيح إلى حاسبك، إذا كان السلك متصلاً بسلك أو منفذ آخر، هذا يعني أن الأمور ليست جيدة.

---

1 البرنامج Sniffer: برنامج يقوم باعتراض البيانات الموجهة عبر الإنترنت وتفحص كل حزمة بحثاً عن معلومات معينة، مثل كلمات المرور المنقولة على شكل نص واضح.

لوحات المفاتيح المراقبة

كشف لوحة مفاتيح تم استبدالها بلوحة مفاتيح مراقبة أصعب بكثير من اكتشاف مسجل مفاتيح مضمن. توجد بعض النقاط المفيدة والمساعدة لاكتشاف هذا النوع من مسجلات المفاتيح:

- **لا تبدو لوحة المفاتيح طبيعية**: إذا اعتقدت لسبب ما أن لوحة المفاتيح لديك تبدو مختلفة قليلاً، عليك توخ الحذر. مثلاً قد يكون اللون مختلف قليلاً، البقع الناتجة عن الأوساخ قد تبدلت، أو أن ملمس المفاتيح قد تغير.
- **استخدام لوحات مفاتيح مرجعية**: في الأيام الغابرة من الإجراءات المضادة للمراقبة التقنية (TSCM) أي technical surveillance countermeasures، تم استخدام الهواتف المرجعية لمقارنة الهواتف التي يشتبه أنها مراقبَة مع الهواتف "النظيفة". حيث كان التقني يختبر أسلاك الدارة بحذر في الهاتف المشتبه لمعرفة وجود أية فروقات بينه وبين الهاتف النظيف. يمكنك تطبيق الطريقة نفسها بفك لوحة المفاتيح، وتبدو رقاقات مسجل المفاتيح التي يستخدمها البائعون واضحة جداً.
- **علامات التغيير**: توجد طريقة بوضع البراغي في زوايا مختلفة وتسجيل الزوايا إما برسم مواقعها أو تصويرها رقمياً. وفي حال قام أحد ما بزرع جهاز مراقبة داخل لوحة المفاتيح فعلى الأرجح أنهم لن يضعوا البراغي إلى مكانها الأول، إلا إذا كان خصمك معقد جداً.

إذا راودك الشك أنك تستخدم لوحة مفاتيح مراقبة، يمكنك ببساطة شراء واحدة جديدة. كما يمكنك أيضاً أن تستخدم لوحة مفاتيح افتراضية على الشاشة المصممة لمستخدمي الحاسب المعاقين، لإدخال نص هام. بما أن مسجل المفاتيح الصلب يتفاعل مباشرة مع لوحة المفاتيح الفيزيائية فإذا استخدمت لوحة مفاتيح افتراضية ستتجنب مسجل المفاتيح. لكن هذه الطريقة لن تجدي نفعاً مع مسجلات المفاتيح البرمجية التي تلتقط صوراً لشاشة العرض، كما أن الجاسوس الذكي سوف يستخدم مسجلات المفاتيح البرمجية والصلبة معاً لتزيد فرص نجاحه في التجسس عليك. كما يتوجب عليك اتباع المقولة الاستخباراتية القديمة، "إذا وجدت جهاز مراقبة ابحث عن غيره".

يقلص استخدام الحاسب المحمول أو لوحة مفاتيح USB، خطر تعرضك للمراقبة باستخدام مسجل مفاتيح، إلا في حالة تعرضك لخصم متطور جداً.

استغلال كلمات مرور مسجل المفاتيح

تستخدم معظم مسجلات المفاتيح البرمجية والصلبة التجارية كلمة مرور أو تتابعاً من المفاتيح، ليتمكن الجاسوس من الوصول إلى الخيارات الإدارية لمسجل المفاتيح. لكن إذا أخطأ الجاسوس

باستخدامه كلمة المرور الافتراضية، التي تعرض غالباً على موقع الويب الخاص بالبائع، يمكنك أنت أيضاً الوصول إلى مسجل المفاتيح.

توجد تقنية فاحصة أخرى وهي كتابة برنامج نصي يعتمد على مهاجمة القوة العمياء للكشف عن وجود مسجل المفاتيح. تميّز معظم مسجلات المفاتيح التجارية تركيب مفاتيح افتراضي أو مدخل من قبل المستخدم والذي يعرض لوحة التحكم الخاصة بمسجل المفاتيح. يمكنك كتابة برنامج نصي بسيط باستخدام لغة البرمجة Visual Basic، Perl، أو أي لغة برمجة أخرى لتجريب جميع تركيبات المفاتيح الممكنة (استخدام المفتاح Ctrl ومفتاحين آخرين).

تستطيع أيضاً كتابة برنامج نصي لتنفيذ مهاجمة القوة العمياء على مسجل مفاتيح صلب وذلك بإرسال جميع تركيبات المفاتيح الممكنة إلى نافذة ومن ثم تسجيل ظهور خرج مختلف عن كلمات المرور التي يتم تجريبها، علماً أن مسجلات المفاتيح الصلبة تستخدم كلمة مرور مدخلة ضمن محرر نصوص لعرض قائمة الأوامر. من الجلي أن هذا الأمر قد يستغرق وقتاً طويلاً جداً إذا كانت كلمة المرور مكونة من أكثر من سبعة محارف.

استخدام نظام التشغيل Linux

أدوات التجسس المماثلة التي تتنصت على مستخدمي نظام التشغيل Linux قليلة جداً، مقارنة مع العدد الكبير من مسجلات المفاتيح المتوفرة على الإنترنت لنظام التشغيل Windows. بالرغم من ذلك يمكن إنشاء مسجل مفاتيح للنظام Linux عن طريق تثبيت نواة معدلة على الحاسب الهدف، لكن هذا المستوى من التعقيد التقني يتجاوز قدرات الجاسوس العادي. على أية حال، تم نشر شيفرة مصدرية لمسجلي مفاتيح على الأقل للنظام Linux. مسجلات المفاتيح هذه بسيطة جداً وإمكانياتها بعيدة عن الميزات التي توفرها مسجلات المفاتيح لنظام Windows. سوف تزداد أدوات التنصت والمراقبة تدريجياً لنظام التشغيل Linux، وخاصة مع ظهور فيروسات جديدة لهذا النظام، وزيادة شعبية هذا النظام وبشكل خاص للاستخدام المكتبي.

إجراءات مضادة: أختام التغيير

إذا كنت تواجه خصماً ممولاً جيداً والذي يريد ضمان عدم كشفه، يوجد دوماً خطر تثبيت مسجل مفاتيح داخل صندوق الحاسب. وهذا الأمر يصعّب كثيراً عملية الكشف لأنه عليك فتح صندوق الحاسب ومن ثم معرفة عما تبحث عنه تماماً. قد تصل بعض العمليات التي تدعمها الحكومة إلى حد أنها ستصنّع رقاقة وحدة تحكم بلوحة المفاتيح والتي تبدو مشابهة تماماً للرقاقة

القياسية لكنها تتضمن أسلاكاً كهربائية تعمل مثل مسجل المفاتيح. (الرجاء أن تتذكر المناقشة في الفصل الأول وإذا كان هذا الأمر محتملاً في حالتك).

من أحد الإجراءات المضادة لمعرفة فيما إذا كان الجواسيس يفتحون حاسبك هو استخدام أختام التغيير، وهي قطع من الشريط المتوضعة فوق المنطقة التي يفتح عندها صندوق الحاسب، فإذا تم فتح الصندوق يمزق الشريط، وبالتالي سيكون لديك دليل أن أحداً ما حاول العبث بحاسبك. قد يستطيع الخصم المحترف التغلب على أختام التغيير، لكنها مع ذلك سوف تجعل عمل الجاسوس أصعب وأكثر استهلاكاً للوقت.

إذا لم تتوفر لديك الكثير من الموارد، يمكنك استخدام بعض الطرق التقليدية الفعالة. افتح صندوق الحاسب، اقتلع بضع شعرات من رأسك ثم احشرها داخل الصندوق عندما تقوم بإغلاقه بحيث يظهر عدد من الشعرات إلى الخارج. فإذا زرع الجاسوس أداة تنصت إلى داخل الصندوق فلن يلاحظ وجود الشعرات. ثم إذا لم تجد الشعرات التي قمت بوضعها هذا يعني قام أحدهم بالعبث بحاسبك.

مراقبة الانهيارات الاستثنائية

مسجلات المفاتيح معرضة للانهيارات مثل أية برمجيات أخرى، وغالباً ما تترك رسائل خطأ غريبة. مع أنه من السهل أحياناً إبعاد الأخطاء في نظام التشغيل Windows، لكن الكثير من مسجلات المفاتيح لا يمكن الاعتماد عليها وقد تسبب أخطاء متكررة للنظام، إذا كنت تشك أنك معرض للتنصت عبر لوحة المفاتيح، راقب رسائل الخطأ في النظام بعد الانهيار لترى إذا كان هناك شيء غريب يحصل.

إجراءات مضادة: جهاز CompuSafe

ابتكرت الشركة الكورية Safe Technology جهازاً يدعى CompuSafe. تقوم بوصل الجهاز إلى منفذ لوحة المفاتيح لديك ومن ثم سلك لوحة المفاتيح إلى الجهاز.

تتضمن العلبة جهازاً للتشفير يتصل ببرنامج تشغيل برمجي، ويجب أن تكون نتيجة هذا نص ممزوج لا يستطيع مسجل المفاتيح البرمجي قراءته (على الأقل مسجلات المفاتيح التي لا تتمتع بميزة التقاط صور لشاشة العرض).

اختبر موقع الويب لشركة ExtremeTech هذا الجهاز ووجدوا أن مسجل المفاتيح WinWhatWhere لا يزال يقوم بتسجيل ضربات المفاتيح بصورة واضحة. لقد نجح هذا الجهاز ضد مسجلات المفاتيح غير المعروفة، لكن عملية إدخال المفاتيح أثناء تنفيذ الجهاز كانت بطيئة جداً.

مع أن هذه الفكرة لا بأس بها، إلا أن تنفيذها يتطلب تصميماً وجهداً إضافياً. يمكنك الاطلاع على مراجعة كاملة للجهاز على الرابط www.extremetech.com/article2/0،3973،472055،00.asp.

إزالة مسجلات المفاتيح

بعد أن تكتشف وجود مسجل مفاتيح على حاسبك وتقرر إما أن تبدأ بحملة تزييف للمعلومات أو قد ترغب بإزالته مباشرة. قد تثبّت مسجلات المفاتيح التجارية الكثير من الملفات على القرص الصلب، ومن الصعب أن تتخلص منها كلياً، لذلك أفضل طريقة هي محاولة تحديد نوع مسجل المفاتيح الموجود لديك. يمكنك تحقيق هذا بإجراء بحث عن طريق الإنترنت باستخدام محرك بحث وإدخال الدليل الذي وجدته مثل أسماء ملفات أو قيم تسجيل. إذا كان مسجل المفاتيح تجارياً تحقق من موقع الويب الخاص به، حيث تزود المواقع تعليمات لإزالة مسجل المفاتيح إلى جانب معلومات أخرى والتي قد تساعدك لتحديد نوعاً محدداً من مسجلات المفاتيح.

إذا لم تتمكن من إزالة مسجل المفاتيح أو لا زلت قلقاً حول وجود نوع آخر من مسجلات المفاتيح على حاسبك، قم بإنشاء نسخة احتياطية للبيانات إلى وسط تخزين جديد، ومن ثم قم بتهيئة القرص الصلب تهيئة بمستوى منخفض، ومن ثم قم بإعادة تثبيت نظام التشغيل من مصدر موثوق (القرص المضغوط الخاص بالبائع). قد يكون هذا الإجراء طويلاً بعض الشيء، لكنها الطريقة المضمونة الوحيدة للتغلب على مسجل مفاتيح برمجي.

تلخيص

تعتبر مسجلات المفاتيح من الأدوات المتداولة والمنتشرة في حقيبة أدوات الجاسوس. لكن من جهة ثانية، يمكن كشف والتغلب على مسجلات المفاتيح البرمجية والصلبة بسهولة نسبية بعد أن تتأكد من وجودها.

- إذا لم تكن تتمتع بخبرة تقنية كبيرة، يمكن أن تستخدم برنامجاً لكشف وجود مسجل المفاتيح، وقم بتحديثه دورياً.
- إذا كانت لديك خلفية تقنية، يمكنك التجريب والبحث عن العمليات الجارية، ونشاطات الملفات التي تحدث، وما هي برامج التشغيل والبرامج التي تنفذ عند بدء تشغيل النظام.

- قم بفحص حاسبك ولوحة المفاتيح عن أية دلالات أو علامات تشير إلى أنه تم زرع مسجل مفاتيح صلب.

ما لم تكن هدفاً لعملية تجسسية معقدة، سوف تخفف هذه الخطوات البسيطة خطر تعرضك إلى المراقبة من قبل مسجل مفاتيح.



التجسس بوساطة تطبيقات حصان طراودة

كثيراً ما نسمع أن التجسس هو ثاني أقدم مهنة في العالم، لذلك قبل أن ندخل في تطبيقات حصان طروادة وعلاقتها بالتجسس الحاسي، سنعود إلى الوراء إلى عالم الأساطير اليونانية من أجل تهيئة المشهد لهذا الفصل.

لنعد إلى القرن الثاني عشر قبل الميلاد، حيث هرب Paris (وهو ابن ملك طروادة) مع Helen، وهي أجمل امرأة على وجه الأرض وزوجة Menelaus ملك إسبرطة. بالتأكيد غضب الملك Menelaus وأخوه الملك اليوناني الجبار Agamemnon غضباً شديداً، وشنا حرباً على طروادة. لكن ولسوء حظ الملك Menelaus كانت المدينة محصنة تحصيناً قوياً ولم يستطع الملك الاستيلاء على طروادة واسترجاع Helen حتى بعد مرور عشر سنوات من الحصار.

أدرك اليونان بعد هذه الفترة من الزمن أنهم لن يستطيعوا الانتصار في الحرب دون استخدام المكر والخداع، لذلك قاموا ببناء حصان خشبي كبير مفرّغ من الداخل، وضعوا مجموعة من الرجال داخله، وتركوه عند بوابة المدينة وركبوا سفنهم للعودة إلى اليونان.

ظن الطرواديون أن هذا الحصان كان علامة السلام وانتهاء الحرب، لذلك سحبوه إلى داخل المدينة المحصنّة وأقاموا حفلاً ضخماً لهذا النصر الذي حققوه. وكما تظن الآن فقد كانت هذه هفوة كبيرة، حيث عندما نام الجميع بعد انتهاء الحفل تسلل اليونانيون إلى خارج الحصان، قتلوا بعض الحراس، وأدخلوا باقي الجيش اليوناني إلى المدينة (الذين رجعوا إلى طروادة بعد حلول الظلام). سقطت طروادة، ذبح جيشها، وأخيراً تمت إعادة Helen.

يستمر ميراث حصان طروادة حتى يومنا هذا على شكل ملفات ورسائل بريد إلكتروني التي لا تكون فعلياً كما تبدو من الخارج. تستطيع تطبيقات حصان طروادة أن تستولي على الحاسب عن بعد عبر الاتصال بشبكة الإنترنت وتسمح للجاسوس أن يسرق الملفات ويتنصت على هدفه

المقصود. يتحدث هذا الفصل عن مبدأ عمل تطبيقات حصان طروادة، كيفية تثبيتها على أجهزة الحاسب، الأنواع المناسبة لعمليات التجسس، والأهم من ذلك كله كيف يمكن كشفها وإزالتها من النظام.

أساليب الجواسيس

سوف تلعب في هذه الفقرة دور مراسل غير أخلاقي لحركة محل تجاري كبير. لقد كنت تعمل في الماضي لصالح جريدة مهمة في العاصمة بعد تخرجك مباشرة من كلية الصحافة في جامعة Colombia. لكن حماسك الزائد أدى إلى كتابة سلسلة من المقالات التافهة حيث قمت بالدمج بين الكتابة الواقعية والروايات، وفي نهاية الأمر طردت من العمل. لقد مررت بأوقات صعبة والأمر الوحيد الذي كان بإمكانك فعله هو التنقيب عن تفاصيل مهينة قذرة حول الفنانين المشهورين. تحول حالياً تجميع مبلغ من المال لقاء ثمن بطاقة طائرة إلى أفغانستان أو إلى مكان ما في الشرق الأوسط. حيث قد تسترجع سمعتك القديمة بقيامك ببعض التقارير الحربية الشجاعة بصفتك مراسل صحفي مبتدئ.

توجد مغنية مشهورة حاول الصحفيون والمصورون تعقبها واكتشاف أمور مشينة عن حياتها لسنوات طويلة. لقد جالت جميع أنواع الإشاعات الفاضحة عنها مثل المخدرات، العلاقات الغرامية، والعنف، لكن لم يستطع أحد الدخول إلى حلقتها الضيقة للحصول على القصة الحقيقية. وقد عرض رئيسك في العمل جائزة بقيمة 50,000 دولار أمريكي لأي شخص يتمكن من جلب معلومات كافية عنها لكتابة تقرير خاص. لذلك فكرت أن هذه الجائزة قد تكفي لثمن بطاقة طائرة إلى عالم الصحافة الحقيقية.

أخوك الأصغر بارع في الحواسب ويقضي ساعات طويلة على خدمة الدردشة IRC (Internet Relay Chat)، يقوم بتحميل البرامج والأغاني، وقد تحول إلى مخرّب صغير (أي أنه يقوم بتحميل موسيقى وبرمجيات غير مرخصة، ويستخدم أدوات مبرمجة من قبل الآخرين لاقتحام الحواسب). وفي يوم من الأيام يطلعك عن تطبيقات حصان طروادة وكيف أنه استطاع اختراق مجموعة من الحواسب ذات نظام التشغيل Windows، والبحث عن الملفات التي تتضمن أرقام بطاقات الاعتماد والإفادات المصرفية. كل ذلك عن طريق إرسال رسائل إلكترونية تتضمن تطبيقات حصان طروادة إلى الأشخاص المغفلين. وفجأة تتذكر أنك حصلت على البريد الإلكتروني الخاص بالمغنية الشهيرة منذ شهرين، وقد كنت محتاراً كيف يمكنك الاستفادة منه، أما الآن فقد تكونت لديك فكرة واضحة عن هذا. وتبدأ بطرح الأسئلة على أخيك حول تطبيقات حصان طروادة.

استغلال نقاط الضعف

تعتمد المهاجمات الناجحة لتطبيقات حصان طروادة على استغلال نقاط الضعف الأمنية ونقاط الضعف البشرية. ويتطلب دخول تطبيق حصان طروادة إلى حاسب الضحية بعض المهارة في الهندسة الاجتماعية وذلك لتقنع ضحيتك على فعل أمر ما يثبّت وينفّذ التطبيق. كما عليك أن تتعامل مع أية دفاعات إلكترونية على حاسب الهدف مثل جدران الحماية، برامج مكافحة الفيروسات، وبرمجيات لمكافحة تطبيقات حصان طروادة.

قد يبدو لك كل هذا مهمة لا تقهر، لكن توجد طرق كثيرة لاستغلال نقاط ضعف مختلفة واستخدام تطبيقات حصان طروادة بشكل فعال لأغراض التجسس. مهاجمات حصان طروادة ضد مستخدمين ساذجين سهلة التحقيق وممكنة حتى ضد المستخدمين الواعين أمنياً لكن مع بعض التفكير والتخطيط.

مقدمة إلى تطبيقات حصان طروادة

حصان طروادة هو تطبيق يبدو أنه رؤوف، لكنه يقوم بدلاً من ذلك بنشاط ضار للنظام. يمكن أن يتنكر تطبيق حصان طروادة على شكل لعبة، ملف مرفق بالبريد الإلكتروني، أو حتى صفحة ويب. بعد أن يقوم الهدف بتنفيذ التطبيق المموه، يقوم تطبيق حصان طروادة بتثبيت نفسه على القرص الصلب ويعمل عند كل بدء تشغيل للنظام Windows.

بعد أن يعمل تطبيق حصان طروادة، يقوم بتنفيذ جميع الأعمال الشريرة التي برمجها صاحبه ليقوم بها. فعلى سبيل المثال، يمكنك باستخدام تطبيق حصان طروادة الذي يعمل على شبكة مفعّلة، أن ترشد هدفك البعيد أن يفتح ويغلق حجرة محرك الأقراص المضغوطة بشكل متكرر، تشغيل الملفات الصوتية، تغيير خلفية سطح المكتب، أو القيام بنشاطات مضحكة أخرى والتي تجعل المستخدم يعتقد أنه قد جن. لكن وبما أن هذا الكتاب ليس "أسرار الحيل الحاسبية"، لنطلّع على بعض الميزات التي تتمتع بها هذه التطبيقات والتي يمكن استخدامها بشكل خاص لأغراض تجسسية، ومن ضمنها ما يلي:

- التقاط خرج بطاقة الصوت والميكرفون.
- التقاط خرج كاميرا الويب.
- تحرير تسجيل النظام.
- الحصول على وتعديل محتويات ملفات بدء التشغيل مثل autoexec.bat و win.ini.
- تعديل الملفات الموجودة.

- تسجيل ضربات المفاتيح.
- استرجاع كلمات المرور المخزنة في الذاكرة المخبئية.
- تنفيذ التطبيقات.
- التقاط صور لشاشة العرض أو استعراض سطح المكتب في الزمن الحقيقي.
- إنهاء العمليات الجارية.
- إلغاء تثبيت التطبيق (إزالة دليل وجود تطبيق حصان طروادة).
- تحميل وإيداع الملفات.

كما ترى، يقدّم تطبيق حصان طروادة بعض الاحتمالات الجدية للجاسوس الذي يريد الحصول على البيانات من مكان بعيد. بعد أن تم تثبيت وتشغيل التطبيق في المكان المطلوب بشكل سري، كل ما تحتاجه الآن هو اتصال بالإنترنت وأداة للتحكم بتطبيق حصان طروادة عن بعد، ويمكنك الوصول إلى الهدف من أي مكان في العالم.

تصنف تطبيقات حصان طروادة عموماً إلى ثلاثة أنواع مختلفة:

- **الوصول المحلي إلى النظام Local System Access**: تم تصميم بعض تطبيقات حصان طروادة الأولى لتحقيق الوصول إلى الأنظمة المحمية. أي مثلاً، قد يقوم مدير نظام Unix بتحميل لعبة شائعة، دون أن يعلم بأنها ستقوم أولاً بالتحقق من أن المستخدم يتمتع بامتيازات الجذر root (أي امتيازات المدير في أنظمة Windows)، وإذا كان كذلك سوف يقوم بإنشاء حساب مدير آخر ذو كلمة مرور معروفة. مثال آخر عن هذا النوع، شاشة تسجيل دخول مزيفة للنظام Windows والتي تقوم بحفظ أسماء الحسابات وكلمات المرور إلى ملف نصي قبل أن تستدعي إجراءات تسجيل الدخول الحقيقية للنظام.
- **تدميرية Vandalism**: بعض التطبيقات مصممة خصيصاً لإلحاق الضرر، مثل حذف الملفات، إعادة تهيئة الأقراص الصلبة، أو أعمال تدميرية أخرى. الاستخدام الوحيد لهذا النوع من تطبيقات حصان طروادة المتعلق بالتجسس هو القضاء على الأدلة.
- **الوصول البعيد Remote Access**: وهو النوع الوحيد المفيد لأعمال التجسس، تسمى أحياناً هذه التطبيقات بالجرذان RATs كاختصار للعبارة (Remote Access Trojans، Remote Administration Tools). تسمح هذه التطبيقات للجاسوس أن يتحكم عن بعد ويتطفل على الحاسب الهدف عبر الشبكة.

من المهم الإشارة إلى أن تطبيقات حصان طروادة لا تقوم بنسخ نفسها بشكل متكرر مثل الفيروسات. أي بعد أن يتم تثبيت التطبيق المحتال على الحاسب، فإنه لا يحاول أن ينشر نفسه إلى حواسب أخرى، وإذا فعل ذلك فإنه يعتبر فيروساً أو دودة. (لكن، يتم نشر الكثير من الفيروسات باستخدام ما يمكن أن يسمى طريقة حصان طروادة، مثل نشر الفيروس عبر ملف مرفق برسالة بريد إلكتروني إلى مستخدم ما. تتم مناقشة الفيروسات المناسبة لأعمال التجسس في الفصل الثالث عشر).

أساليب: لا تثق بأحد

مع أن أحصنة طروادة موجودة منذ أيام Helen، لكن ظهر أحد الأمثلة الأولى المنشورة عن مخاطر إصدارات الأيام الحديثة في عام 1984، من قبل Ken Thompson، أحد المطورين الأصليين للنظام UNIX.

وصف Thompson هجوماً حيث يتم تعديل الشيفرة المصدرية لمترجم C بحيث كل مرة يتم فيها ترجمة الشيفرة الخاصة بأمر تسجيل الدخول للنظام UNIX، سيتعرف المترجم على الشيفرة المصدرية ومن ثم يغيرها بإضافة سطور جديدة تقوم بإنشاء كلمة مرور إضافية (خفية) إلى الخرج الثنائي.

وبالتالي أي شخص استخدم المترجم لإنشاء أمر تسجيل الدخول سيصنع دون أي علم إصداراً يجعل النظام معرّضاً لأي شخص يعلم بوجود كلمة المرور الإضافية. وقد تم تفتيش الشيفرة المصدرية لتسجيل الدخول بدقة تامة، ولم يتم إيجاد أي دليل عن وجود حصان طروادة.

اقترح Thompson أنه من خلال جعل الخرج الثنائي الذي خضع لتأثير تطبيق حصان طروادة، مترجم لغة C الافتراضي لتوزيعات UNIX، سوف يظهر الباب الخلفي لأمر تسجيل الدخول في كثير من الأنظمة حيث قام المستخدم بإعادة ترجمة نظام التشغيل. كان مغزى Thompson هو، "لا يمكنك الوثوق بشيفرة لم تقم أنت بإنشائها كلياً." (تتوفر المقالة الأصلية المكتوبة لمحاضرة منح الجوائز في Turing على الرابط /www.acm.org/classics/sep95).

لا تزال مراقبات Thompson صالحة للتطبيق إلى يومنا هذا، هذه الأحداث في النصف الثاني من عام 2002:

- في شهر تشرين الثاني (نوفمبر)، اكتشف أحد الأشخاص الشيفرات المصدرية الحديثة للبرامج libpcap
و tcpdump من الموقع tcpdump.org، وقد تضمنت إصداراتها البديلة تطبيق حصان طروادة.
- ما بين 28 أيلول (سبتمبر) و 6 تشرين الأول (أكتوبر)، انتشر تطبيق حصان طروادة في الشيفرة المصدرية لتطبيق Sendmail 8.12.6.

- في شهر آب (أغسطس)، اخترق أحد ما أمن الموقع ftp.openbsd.org وقام بتثبيت تطبيق حصان طروادة في الحزمة مفتوحة المصدر OpenSSH.
- في شهر حزيران (يونيو)، تم اقتحام موقع الأمن monkey.org لشركة Dug Song، واستبدل أحدهم الشيفرات المصدرية dsniff، fragroute، و fragrouter بإصدارات خضعت لتطبيق حصان طروادة.

من الممكن أيضاً إضافة تطبيقات حصان طروادة إلى الخرج الثنائي لنظام التشغيل Windows عن طريق تطبيق الهندسة العكسية وإعادة ترجمة النظام (تتم مناقشة هذا الموضوع لاحقاً في الفصل الثالث عشر).، بالرغم من أن بعض مناصري النظام Windows سيعتبرون هذا الأمر تهمة أمنية للبرمجيات مفتوحة المصدر.

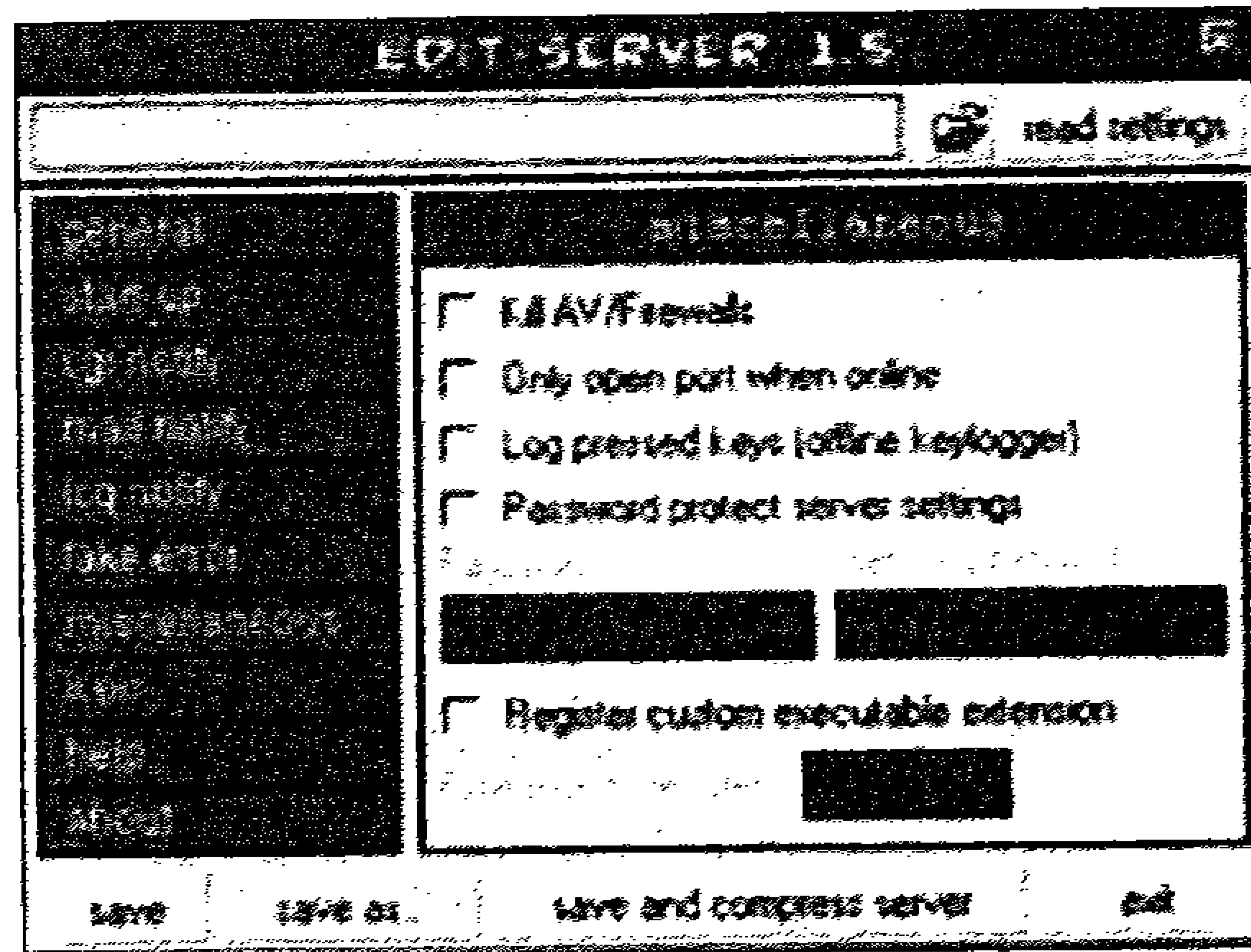
مبدأ عمل تطبيقات حصان طروادة

يوضح لك أخوك الصغير أن جميع تطبيقات حصان طروادة تقريباً تعمل بنفس الطريقة. يقوم المستخدم بشيء ما عن غير قصد مما يؤدي إلى تخزين التطبيق على قرصه الصلب. قد يكون هذا الفعل إما فتح ملف مرفق برسالة بريد إلكتروني، استعراض صفحة ويب، أو تنفيذ تطبيق قام بتحميله من شبكة الإنترنت. بعد أن يتم تثبيت تطبيق حصان طروادة، يتم تنفيذه مباشرة أو يقوم بالتنفيذ بعد إعادة تشغيل الحاسب، كما يتم تعديل التسجيل أو أي ملف بدء تشغيل آخر ليتم تنفيذ تطبيق حصان طروادة عند إقلاع النظام Windows.

سوف نركز بشكل أساسي على مبدأ عمل تطبيقات حصان طروادة ذات الوصول البعيد، لأنها تحمل إمكانيات لا بأس بها في عمليات التجسس. وعموماً، يتألف تطبيق حصان طروادة من ثلاثة مكونات: الملقم server، العميل client، ومحرر الملقم server editor:

- **الملقم server**: الملقم هو التطبيق المثبت على الحاسب البعيد المستهدَف ويقوم بالمراقبة الفعلية. تتمتع الملقمات المختلفة بخصائص مختلفة، تتراوح من ملقم يبلغ حجمه عدة مئات من الكيلو بايتات والتي يمكن أن تفعل أي شيء قد يخطر لك، إلى ملقمات صغيرة تسمى مودعات "uploaders" والتي قد يبلغ حجمها 20KB فقط وهذا ما يجعلها غير مثيرة للشكوك مقارنة مع الملقم الذي يبلغ حجمه 200KB عند محاولة التسلل إلى النظام الهدف باستخدام هذا الملقم. يُستخدم المودع للحصول على موطئ قدم على الحاسب الهدف، ومن ثم يقوم، كما يظهر من اسمه، بإيداع ملقم حصان طروادة أكبر ذو خصائص أكثر. بعد تنفيذ أي ملقم، يفتح منفذاً في الحاسب ويستمع ومن ثم ينفذ الأوامر. الملقمات الأصغر دوماً أفضل، لأغراض التجسس، يمكنك على الأقل الحصول على ملقم يقوم بتحميل الملفات من الحاسب الهدف ربما يقوم بتسجيل ضربات المفاتيح.

- **العميل client**: يرسل تطبيق العميل الأوامر إلى الملقم ويستقبل البيانات منه. تقوم بإدخال عنوان IP لهدفك ضمن تطبيق العميل، وإذا كان الملقم في حالة تنفيذ والاتصال مهيأ عبر منافذ محددة، يتم بعد ذلك تمرير حزم TCP وUDP بين التطبيقين. يستخدم عدد لا بأس به من تطبيقات حصان طروادة نوعاً من التشفير للبروتوكولات التي تستخدمها وذلك لإخفاء محتويات الاتصالات بين الملقم والوكيل. تتمتع معظم تطبيقات العميل بواجهات سهلة الاستخدام جداً، لذلك ليس من الضروري أن تقوم بإرسال سلاسل محرفية غامضة لينجح الاتصال مع الملقم.
- **محرر الملقم Server editor**: المكون الأخير لتطبيق حصان طروادة ذو الوصول البعيد هو محرر الملقم (انظر الشكل 1-9). يستخدم هذا البرنامج لإعداد الملقم قبل أن يتم استخدامه، تسعى معظم الملقمات أن تكون قابلة للتكوين والإعداد بسهولة، ويمكنك تحديد بعض الخيارات مثل اسم الملف الذي ترغب منحه للملقم، أرقام منافذ الاتصال، كيف يبدأ تنفيذ الملقم، وكلمة مرور الملقم (بحيث تستطيع أنت فقط الوصول إلى الملقم).



الشكل (1-9) محرر الملقم لتطبيق حصان طروادة NetDevil، يظهر خيارات تكوين متنوعة.

قبل أن تتمكن من إرسال الأوامر من العميل إلى الملقم، يجب أن تعرف عنوان IP للحاسب الهدف، وعندما يتم تنفيذ الملقم يقوم بالاستماع إلى منفذ محدد. لذلك تحتاج إلى عنوان IP للهدف لتتمكن من تكوين اتصال مع الملقم. (تستخدم بعض التطبيقات منافذ افتراضية أو محددة مما يجعلها سهلة الكشف. يقوم المخربون خلال فحص المنافذ، التي سوف نناقشها بالتفصيل في الفصل العاشر، بالبحث عن المنافذ المستخدمة بصورة شائعة من قبل تطبيقات حصان طروادة محاولين اكتشاف الأنظمة التي تم اختراقها مسبقاً من قبل هذه التطبيقات (هذا الأمر يوفر عليهم

جهد تثبيت تطبيقات حصان طروادة الخاصة بهم). مثلاً إذا كشف فحص المنافذ المنفذ الفعال ذو الرقم 27374، فمن المحتمل جداً أن يكون الحاسب قد تعرض لتطبيق حصان طروادة Sub7 والذي يستخدم ذلك المنفذ بشكل افتراضي).



شكّل Mikael Simovits لائحة شاملة لتطبيقات حصان طروادة والمنافذ التي تستخدمها، يمكنك الإطلاع عليها من خلال الرابط:
www.simovits.com/nyheter9902.html.

هناك عدة طرق لمعرفة عنوان IP للحاسب الهدف، وقد تحصل بعض الملقمات عليه عند تنفيذها من خلال استخدام رسالة إلكترونية، رسالة تنبيه عبر خدمة ICQ، أو برنامج نصي CGI على صفحة ويب ليعلمك عن عنوان IP للحاسب الهدف.

يمكن أن تبرمج الملقمات افتراضياً باستخدام أي لغة برمجة، وتوجد العديد من المصادر على شبكة الإنترنت إذا أردت برمجة ملقم خاص بك. الملقمات المبرمجة باستخدام اللغات assembly و C/C++ أصغر حجماً وأكثر خفية من الملقمات التي تمت برمجتها باستخدام لغات برمجة أعلى مثل Visual Basic (من جهة ثانية لغة البرمجة عالية المستوى Delphi شائعة جداً بين مبرمجي تطبيقات حصان طروادة)، لكن مع ذلك توجد طرق عديدة لتقليص حجم الملف التنفيذي لجعله أقل وضوحاً.

خطر: تطبيقات حصان طروادة الدولية

أرسلت وزارة الخارجية الأمريكية، في الثاني من شهر شباط (فبراير) عام 2000، برقية عاجلة إلى 170 سفارة حول العالم تتضمن أمراً بإزالة برنامج خاص بالميزانية من جميع الحواسب خلال خمسة أيام.

حيث تمت تقوية الإجراءات الأمنية منذ بضع أشهر، في أعقاب اعتقال دبلوماسي روسي اشتبه بالتجسس على رؤساء الوزارة. ومن ثم أصيب أحدهم بالقلق حول الحزمة البرمجية التي طورتها شركة Synergy International Systems التي تم استخدامها لتخطيط الميزانية والتخطيط الاستراتيجي.

وقد اكتشفت القوة الأمنية الدبلوماسية لوزارة الخارجية الأمريكية، أن معظم الموظفين في شركة Synergy من الاتحاد السوفييتي سابقاً، كانوا يقومون بزيارة مكاتب الوزارة بصورة دورية كجزء من عملية استخدام البرنامج بصورة فعالة. حيث منحت وزارة الخارجية عقداً

بقيمة مليون دولار أمريكي إلى الشركة لتقوم بتطوير وتثبيت برمجيات لمعالجة البيانات غير سرية لكن بالغة الدقة.

بدأت عملية تطوير التطبيق في منتصف التسعينيات في السفارة الأمريكية في موسكو، ونال التطبيق قبولاً كبيراً من قبل الموظفين حتى تم استخدامه في جميع السفارات الأمريكية حول العالم. كان هذا إنجازاً هاماً في حياة Ashot Hovanesian، وهو من أصل أمريكي والمبرمج الأصلي الذي خطا نحو تأسيس شركة Synergy.

صرحت المذكرة الصادرة عن وزارة الداخلية، في الأول من شهر شباط (فبراير) عام 2000، أن الهدف من التحقيقات هو، "محاولة تحديد أية شيفرة برمجية قد تساعد على تشغيل تطبيق حصان طروادة، فيروس، أو أي نوع آخر من الشيفرة الخبيثة." وقد تولى كل من مكتب التحقيقات الفدرالي ووكالة الأمن القومي تحقيقاً لمكافحة التجسس وفحصوا الشيفرة المصدرية للتطبيق والمؤلفة من مليون سطر برمجي وذلك لضمان أن كل شيء طبيعي. كما أن التحقيقات لم تكشف أبداً أي انتهاكات صادرة عن الشركة، وهي من جهتها لا تزال تقوم بتطوير منتجات قواعد بيانات للمهام الصعبة.

تكررت حادثة مماثلة في شهر كانون الأول (ديسمبر) عام 2002، عندما قام مكتب التحقيقات الفدرالي بإجراء تحقيقات حول شركة Ptech وهي شركة لتطوير البرمجيات في Massachusetts. تلقت هذه الشركة عرضاً مغرياً من رجل أعمال سعودي، ياسين القاضي. وتبين من وكالات الاستخبارات الحكومية عن وجود شكوك حول ارتباط القاضي بتمويل منظمات مختلفة وخاصة تنظيم القاعدة. وقد صرحت وسائل الإعلام عن احتمال أن المنتجات البرمجية المستخدمة من قبل الحكومة والمؤسسات التجارية Fortune 1000 تحوي تطبيقات حصان طروادة مزروعة من قبل بن لادن.

برأت الحكومة شركة Ptech من جميع الاتهامات، في منتصف كانون الأول (ديسمبر) عام 2003، لكنها تحولت نتيجة هذا من شركة مثمرة تحوي 65 موظفاً إلى شركة لا تحوي أعمالاً جديدة وتقلص عدد الموظفين لديها إلى عشرة.

كيف تتجنب تطبيقات حصان طروادة الكشف

ليقوم تطبيق حصان طروادة بمهمته بنجاح، يجب أن يتجنب الملقم الكشف على مستويين مختلفين: المستخدم الذي يفحص النظام يدوياً والبرامج الخدمية المصممة لكشف تطبيقات حصان طروادة (سوف نشرح تقنيات وأدوات كشف معينة في فقرة "الإجراءات المضادة" لاحقاً من هذا الفصل).

يتجنب الجواسيس وتطبيقات حصان طروادة الكشف من قبل المستخدم باستخدام بعض الطرق منها:

- **استغلال الثقة:** إذا استقبلت رسالة إلكترونية من شخص تعرفه فإنك على الأغلب سوف تفتح الرسالة مقارنة مع رسالة مجهولة المصدر. استخدم هذا الأمر لصالحك واكتب رسالة وكأنها مرسلة من مصدر موثوق والتي تتضمن ملفاً مرفقاً لتطبيق حصان طروادة أو تتضمن رابطة إلى موقع ويب يقوم بتثبيت التطبيق. (قد تكون هذه بداية لتثبيت تطبيق حصان طروادة على حاسب مغنية ما).
- **الملفات المموهة:** قد يتمتع بعض المستخدمين بذكاء كاف لكي لا يفتحوا ملفاً تنفيذياً (ذو اللاحقة exe.)، لذلك يمكنك إخفاء نوع الملف. أحد طرق القيام بهذا الأمر هو حشو اسم الملف بفراغات إضافية، مثلاً: pics.jpg——————————————————exe.، حيث تمثل علامات الترقيم – فراغاً. والآن تكون قد حصلت على اسم ملف طويل جداً بحيث لن يستطيع تطبيق البريد الإلكتروني عرضه كاملاً أي لن يرى المستخدم اللاحقة الحقيقية للملف، إنما سوف يعتقد أنه ملف صورة عادي. يعاني عدد من تطبيقات البريد الإلكتروني الشائعة مثل Outlook Express وMicrosoft Outlook من عدد من المساوئ التي يمكن استغلالها لتمرير تطبيق حصان طروادة كملف عادي.
- **استخدام منفذ غير مرتبط بتطبيقات حصان طروادة الأخرى:** تستخدم معظم تطبيقات حصان طروادة منافذ افتراضية لإنشاء الاتصال بين الملقم والعميل، كما توجد لوائح منتشرة بشكل واسع لأرقام هذه المنافذ، ويستطيع المستخدم الذكي استخدام الأمر netstat -a أو برنامج لعرض المنافذ لمعرفة إذا كان هناك أية منافذ مفتوحة وموجودة في اللائحة. إذا كان تطبيق حصان طروادة الذي تستخدمه يملك خاصية لتغيير رقم المنفذ يمكنك اختيار رقم فريد غير موجود ضمن اللائحة (لا تتعارض المنافذ ذات الأرقام الكبيرة عادة، مع الخدمات القياسية للنظام والتي تستخدم منافذ ذات أرقام صغيرة).
- **الاختباء في لائحة المهام:** تخفي معظم تطبيقات حصان طروادة وجودها ضمن لائحة مدير المهام، تماماً مثل مسجلات المفاتيح التي ناقشناها في الفصل الثامن. لكن هذا أمر أصعب قليلاً في أنظمة التشغيل Windows 2000/XP، حيث يجب أن تسمي برنامج الملقم بحيث يبدو وكأنه جزء من نظام التشغيل. إذا تفحص المستخدم المرتاب لائحة العمليات الجارية في تسجيل النظام أو مجلد بدء التشغيل، فقد يظن أن تطبيق حصان طروادة هو خدمة عادية في النظام. لذلك يمكنك مثلاً تسمية عملية تطبيق حصان طروادة بالاسم Explorer.exe، وهي قريبة جداً من اسم العملية الأصلية explorer.exe (بالحرف الصغير) لتجنب الكشف من قبل كثير من المستخدمين.

يتطلب التغلب على أدوات الكشف المؤتمتة حذراً ومهارات تقنية إضافية، توجد بعض الطرق منها:

- **تطوير ملقم جديد:** ينشر الكثير من المطورين الأصليين لتطبيقات حصان طروادة الشيفرة المصدرية لإبداعاتهم، لذلك من السهل جداً تطوير تعديل لأحد هذه التطبيقات، أو تجميع أجزاء مختلفة من تطبيقات مختلفة لتوليد تطبيقك الخاص إذا كنت تتمتع ببعض المهارات البرمجية. حيث تملك تطبيقات حصان طروادة الفريدة فرصة كبيرة لتتجنب الكشف من قبل برامج مكافحة الفيروسات أو مكافحة تطبيقات حصان طروادة. لكن قبل أن تبدأ باستخدام تطبيقك المنجز بجهدك الشخصي، يجب أن تختبره ضد الإصدارات الحالية من برامج الكشف الشائعة.
- **تعديل الملقم الأصلي لكي لا يتطابق مع رقم التعريف (وهو رقم وحيد يُضمّن في البرمجيات أو التجهيزات لأهداف توثيقية بحتة):** تبحث برامج مكافحة الفيروسات وتطبيقات حصان طروادة على تسلسل محدد من البايتات أو قيم محددة للمجموع التدقيقي في الملفات المطابقة لتطبيقات حصان طروادة. يمكنك باستخدام محرر ست عشري تعديل البايتات التي لن تؤثر على وظائف التطبيق، قد لا يتم كشف ملقم تم تغييره.
- **ضغط الملقم:** عند بدء تنفيذ الملقم يمكن استخدام برنامج ضغط يقوم بتقليص حجمه وبالتالي يصعب كشفه من قبل برامج الكشف عن طريق طول الملف أو تسلسل البايتات.
- **تقييد الملقم بتطبيق آخر:** توجد تطبيقات تسمى exe binders. (executable binders) تستطيع أن تربط تطبيقين أو أكثر إلى ملف تنفيذي وحيد. عندما يتم تنفيذ التطبيق المربوط ستنفذ باقي التطبيقات المرتبطة أيضاً. يمكنك باستخدام تطبيق الربط هذا تقييد تطبيق حصان طروادة مع تطبيق آخر موثوق بسهولة.

وسائل التجارة: Compressors، Binders، و Droppers

إذا بدأت بالاختلاط بمجتمع حصان طروادة على الإنترنت، غالباً سوف تسمع بثلاثة مصطلحات: Compressors، Binders، و Droppers. وهي أدوات هامة جداً لمعلومات المستخدم والتي يجب أن تعرفها.

Compressor وهو برنامج خدمي يقوم بتقليص حجم ملف تنفيذي (exe.). ويختلف Compressor عن بقية برامج الضغط العادية أنه يمكن تنفيذ الملف المضغوط دون الحاجة إلى فك ضغطه أولاً. أدوات Compressor شائعة جداً بين مستخدمي تطبيقات حصان طروادة لتقليص

حجم الملقم إلى جانب إخفاءه من برامج الكشف التي تبحث عن حجم محدد أو أي رقم تعريف آخر. أحد أدوات الضغط Compressor المعروفة هي UPX (Ultimate Packager for Executables)، وتتوفر على الرابط http://upx/sourceforge.net. بالرغم من أن هذه الأدوات لم تكن مصممة لأغراض خبيثة، إلا أن معظمها يحوي تنسيق ملفات فريد يمكن أن يكشف من قبل برامج مكافحة تطبيقات حصان طروادة.

Binder: هي أداة سهلة الاستخدام تقوم بربط تطبيق أول بتطبيق آخر أو أكثر، وعندما يتم تنفيذ التطبيق المرتبط تُنفّذ جميع التطبيقات المرتبطة. هذه الأداة جيدة لربط تطبيق حصان طروادة مع تطبيق آخر معروف. من أحد مساوئ هذه التقنية أن الترويسات التي تضعها الأدوات Binder الشائعة في الملف المرتبط معروفة من قبل برامج الكشف وسوف تكتشفها. للحصول على لائحة من الأدوات Binder اتبع الرابط www.tlsecurity.net/exebinder.htm.

Dropper: وهو تطبيق يتضمن شيفرة تقوم سرياً بتثبيت وتنفيذ تطبيق حصان طروادة. مثال تقليدي عن مثل هذا التطبيق هو لعبة Whack-A-Mole والتي انتشرت على شبكة الإنترنت عام 1998. مع أن التطبيق كان يبدو لعبة مسلية لكنه في الحقيقة كان يثبّت تطبيق حصان طروادة NetBus.

يتوفر الكثير من تطبيقات Dropper مع الشيفرة المصدرية على الرابط:
www.megasecurity.org/Droppers.html.

تثبيت تطبيقات حصان طروادة بشكل خفي

لقد ارتأينا عزيزي القارئ وضع هذه الفقرة ضمن موقعنا على الإنترنت: http://www.raypub.com. لذا، نتمنى منك العودة إلى الموقع لقراءة هذه الفكرة من صفحة الكتاب ضمن بند "أفكار وتقنيات".

وسائل التجارة: تطبيقات HTML HTAs

يدعم برنامج Internet Explorer ما يعرف باسم تطبيق HTML (HTA، HTML Application). تطبيق HTML هو ببساطة ملف HTML له اللاحقة HTA.. يمكن أن يتضمن تطبيق HTML، أوراق نمط متتالية، وشيفرة مكتوبة باستخدام لغات برمجة نصية مختلفة. عندما يصادف النظام Windows تطبيق HTML فإنه يتعامل معه كأي ملف تنفيذي.

يمكن أن يشير الاختصار HTA أيضاً إلى Heavy Trojan Action وإليك السبب في ذلك. عندما أعلن Georgi Guninski، وهو إنسان باحث عن نقاط الضعف الأمنية في منتجات شركة

Microsoft، أنه يمكن أن تثبت صفحة ويب مُهيأة بشكل محدد تطبيق HTML على حاسب بعيد إذا تم استعراض الصفحة باستخدام برنامج Internet Explorer. وسرعان ما بدأ مبرمجو تطبيقات حصان طروادة بصنع الأدوات للاستفادة من نقطة الضعف هذه. توجد أدوات مثل GodWill، GodMessage، و ExeToHTML تقوم بحشر تطبيق حصان طروادة إلى الشيفرة المصدرية لصفحة الويب كنص ست عشري. عندما يتم عرض الصفحة يتحول تطبيق حصان طروادة من نص إلى تطبيق HTML (HTA) ويتوضع ضمن مجلد بدء التشغيل. تقع جميع هذه الأحداث دون أي علم من قبل المستخدم. يتم تنفيذ تطبيق حصان طروادة عند التشغيل التالي للنظام. (يمكن تطبيق هذه الميزة مع برامج Outlook/Outlook Express حيث يتم تضمين تطبيق HTML ضمن رسالة إلكترونية ذات تنسيق HTML).

استجاب معظم بائعي برمجيات مكافحة الفيروسات إلى هذه السيئة وقاموا بتحديث منتجاتهم لتكشف تطبيقات HTML المثبتة سرياً، كما أصدرت شركة Microsoft أيضاً سلسلة من الترميمات الأمنية لمواجهة هذه المشكلة. لكن من جهة ثانية، إذا أمكن تعطيل برنامج مكافحة الفيروسات بشكل سري وإذا لم يحوي الحاسب الهدف الترميمات الأمنية الحديثة (وهو أمر شائع جداً)، قد يكون هذا الهجوم فعالاً.

يمكنك الاطلاع على بعض التفاصيل عن تطبيقات HTML من شركة Microsoft، على الرابط http://msdn.microsoft.com/workshop/author/hta/overview/htaoverview.asp، بينما يصف الموقع الخاص بالباحث Guninski على الرابط www.guninski.com، ثغرة عنصر التحكم ActiveX (Scriptlet.typelib) بالإضافة إلى ثغرات Microsoft الأخرى التي يمكن استخدامها لأغراض التجسس.

أدوات حصان طروادة

لقد أصابك الملل من المعالجة الطويلة وأخيراً تقول لأخيك "أظهر هذه التطبيقات!"، يشرح لك أن هناك آلاف من تطبيقات حصان طروادة على شبكة الإنترنت، ما رأيك أن تختار أحدها والتي تناسب احتياجاتك التجسسية، لكن هذا يعتمد على هدفك والإجراءات الأمنية التي لديه، وكلما زادت إجراءات الحماية الأمنية زادت مدى خفية الملقم وطريقة استخدامه. (قد تضطر في بعض الحالات استخدام أنواع مختلفة من تطبيقات حصان طروادة، وذلك في حال تم اكتشافها لن يكون الأمر واضحاً فيما إذا كان الملقم قد ثُبت على الحاسب من قبل جاسوس أو من قبل هاوٍ يريد التلاعب فقط).

قبل أن تنشر تطبيق حصان طروادة، يجب أن تختبره لتتأكد من أنه يناسب احتياجاتك، لكن توخى الحذر لأنك تلعب بالنار. فإذا لم تتوفر لديك الشيفرة المصدرية و لم تقم بتكوين التطبيق بنفسك، فلن تعرف أبداً ماذا وضع المبرمج داخل الملقم والعميل ومحرر الملقم (لكن قد تتفاجأ

إذا علمت عن وجود كمية كبيرة من الشرف بين مطوري تطبيقات حصان طروادة، حيث تلعب سمعة المبرمج دوراً كبيراً في البنية الاجتماعية). أما الآن اتبع الإرشادات التالية:

- اختيار نوع تطبيق حصان طروادة الذي تريد استخدامه على حاسب مكوّن بشكل مشابه لحاسب الهدف.
- إذا كنت لا تعرف نوع برنامج مكافحة الفيروسات أو تطبيقات حصان طروادة المثبت على حاسب الهدف، قم بتثبيت الإصدارات الشائعة واختبر التطبيق ضدها جميعاً. بعد أن تقوم بتشغيل الملقم جرّب تطبيق بعض الإجراءات المضادة المعروضة في نهاية الفصل لتعرف إذا كنت سوف تكشف التطبيق.
- تطبيق جميع هذه الاختبارات على حاسب معزول عن بقية الشبكة، لكي لا تتضرر بقية الحواسب عن طريق الخطأ. كما يجب أن تثبت برامج أمنية كافية على حاسبك لمنع تطبيق حصان طروادة من الانقلاب ضدك.
- إعادة تهيئة القرص الصلب لحاسب الاختبار بعد الانتهاء لضمان عدم وجود أية آثار متبقية من شيفرة التطبيق.

والآن لنلقي نظرة على بعض تطبيقات حصان طروادة التي يمكن استخدامها للتجسس. يمكن تقسيم هذه التطبيقات إلى ثلاث فئات: التطبيقات التقليدية وهي الأولى على الساحة وظهرت منذ عدة سنوات (وانتشرت كثيراً)، الجيل القادم من تطبيقات حصان طروادة وهي ليست معروفة مثل سابقتها لكنها أكثر خفية منها، وأخيراً المنتجات التجارية المصممة لإدارة الشبكة لكن يمكن أن تخدم كتطبيقات حصان طروادة.

تطبيقات حصان طروادة التقليدية

ظهرت تطبيقات حصان طروادة ذات الوصول البعيد لنظام التشغيل Windows في أواخر التسعينيات، مترافقة مع تغطية واسعة من قبل وسائل الإعلام. وفي الفقرات التالية وصف لبعض تطبيقات حصان طروادة الهامة الأولى:

NETBUS: وهو تطبيق حصان طروادة الشائع الأول للوصول البعيد، كما أنه سهل الاستخدام ومصمم لنظام التشغيل Windows. قام بتطويره Carl-Fredrik Neikter ونُشر في آذار (مارس) عام 1998. لقد انتشر استخدام هذا التطبيق في الوقت الذي أُطلق تطبيق حصان طروادة Back Orifice (انظر الفقرة التالية)، لكنه لم يحظى بنفس القدر من الشعبية. لقد كانت الإصدارات الأولى من تطبيق NetBus أكبر بكثير من التطبيق BO، لكنها كانت تنفذ على أنظمة التشغيل Windows NT/2000. اجتاز تطبيق حصان طروادة NetBus سلسلة من

التحديثات وتطور أخيراً إلى منتجات مراقبة تجارية وهي المنتجات المعروفة حالياً باسم Spector وeBlaster، والتي تباع من قبل شركة SpectorSoft (www.spectorsoft.com). لا تزال الإصدارات الأصلية للتطبيق NetBus متوفرة على الإنترنت، ويمكنك إيجادها بسهولة بإجراء بحث على المحرك Google.

BACK ORIFICE: أطلقت مجموعة القراصنة Cult of the Dead Cow (cDc) في صيف عام 1998، تطبيق Back Orifice (BO)، وهو تطبيق حصان طروادة ذو الوصول البعيد كان ينفذ على أنظمة التشغيل Windows 95/98 (www.cultdeadcow.com/tools). روّجت مجموعة cDc هذا الهجوم ببراعة وجذبت الكثير من الاهتمام من قبل وسائل الإعلام إلى التهديد الذي يشكله تطبيق حصان طروادة البعيد. بعد مرور سنة تقريباً، أطلقت المجموعة cDc إصدار BO ليعمل ضمن بيئة النظام Windows 2000 (BO2K). ثم تحول BO2K في نهاية الأمر إلى مشروع مفتوح المصدر بصفته أداة شرعية لإدارة النظام أكثر منه تطبيق حصان طروادة، ولا يزال تطويـــره جاريـــاً. لتحميـــل الأداة وللحصـــول على مزيـــد من المعلومـــات اتبع الرابـــط .http://bo2k.sourceforge.net

SUB7: تمت برمجة وإصدار هذا التطبيق من قبل MobMan في نهاية عام 1999، وقد أصبح Sub7 بعد فترة قصيرة أكثر التطبيقات انتشاراً واستخداماً. تمتع التطبيق بميزات متنوعة من ضمنها القدرة على إعلام الملقم ليفحص وجود ضحايا آخرين لهذا التطبيق. ومن ثم تم إصدار عدد من النسخ المحدثة ولا يزال استخدامه شائعاً جداً. تتوفر جميع هذه الإصدارات، من بينها الإصدار Defcon والذي يعتبر الأكثر ثباتاً، على الرابط:

www.megasecurity.org/trojans/subseven/Subseven_all.html.

تطبيقات الجيل القادم لأحصنة طروادة

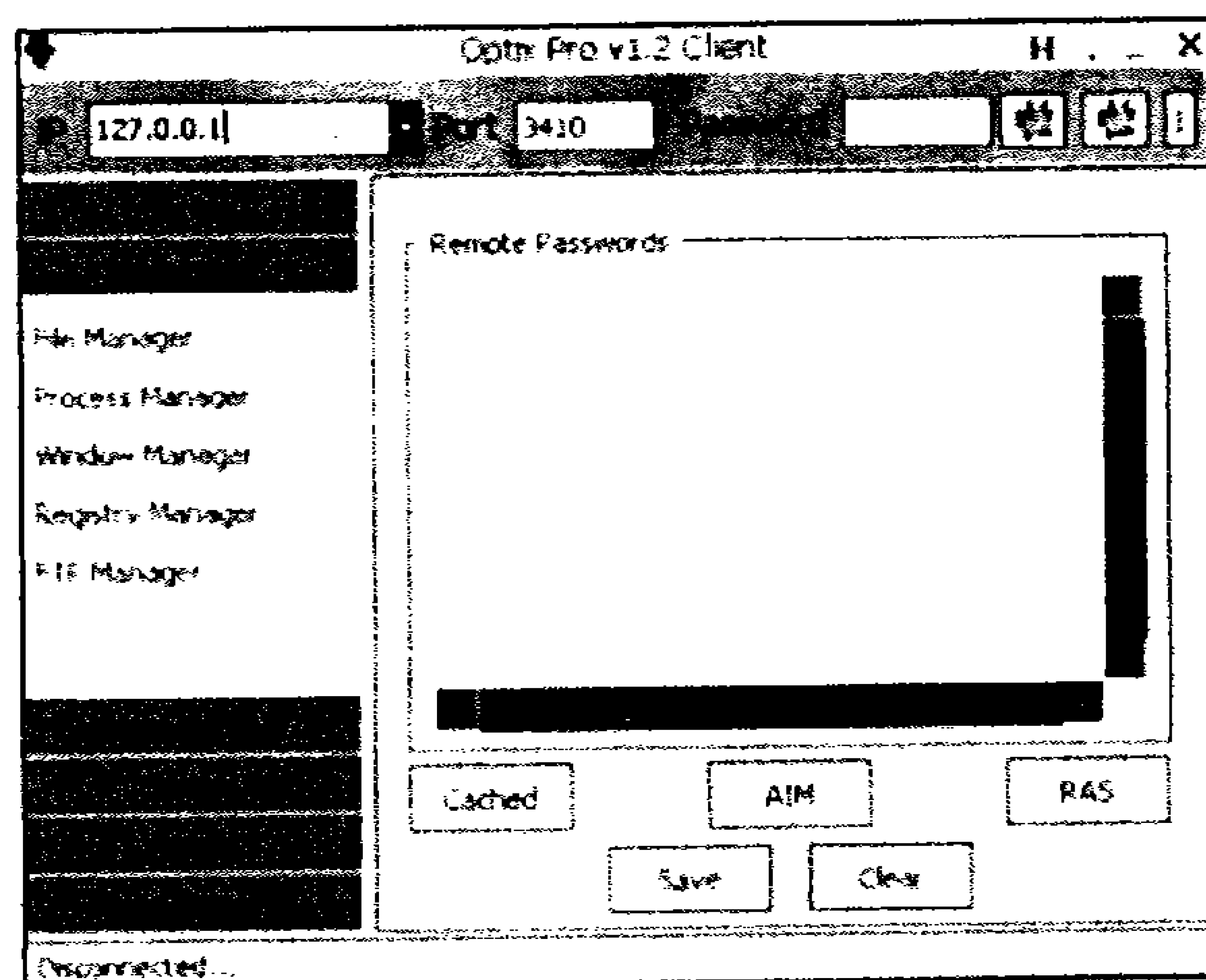
تتمتع تطبيقات حصان طروادة العصرية بمزايا مشتركة مع أجدادها التقليدية، لكنها أكثر تعقيداً من سابقتها وأكثر قوة. حيث يخضع المطورون لتطبيقات حصان طروادة لمعركة متصاعدة مع بائعي برمجيات الأمن عن طريق إيجاد ميزات جديدة مثل إمكانية تعطيل جدران الحماية وبرمجيات مكافحة الفيروسات، عن طريق توليد رسائل خطأ مزيفة لإخفاء نشاطهم وجاعلين عملية الكشف والإزالة أكثر صعوبة، وإشاعة أن الحاسب الهدف يعمل على البريد الإلكتروني أو خدمة دردشة.

وفي الفقرات التالية وصف لبعض تطبيقات حصان طروادة التي يمكن الاستفادة منها في أعمال التجسس.

LANFILTRATOR: من أحد التحديات التي تواجه مستخدم تطبيق حصان طروادة هي الحالة التي يكون فيها الحاسب الهدف متصل بموجّه Router، لن تفيد عناوين IP الداخلية للشبكة المحلية كثيراً في محاولتها الاتصال بالملقم. يعتبر LANfiltrator أحد تطبيقات حصان طروادة الأولى التي تعمل بصورة عكسية، حيث بدلاً من قيام العميل بالاتصال بالملقم، يقوم الملقم بعد أن يصبح فعالاً بمحاولة الاتصال بالعميل. التطبيق مبرمج من قبل Read101 ويتوفر على الرابط www.digitalsin.net/cyn/HTML_/News.html.

OPTIX: التطبيق مطور من قبل شركة EES (Evil Eye Software) ويوجد منه إصداران هما: small Optix Light وfull-featured Optix Pro (انظر الشكل 2-9، والذي يظهر واجهة عميل التطبيق Optix Pro). الإصدار Light مفيد للحصول على موطئ قدم في النظام، أما الإصدار الاحترافي Pro يتضمن جميع الميزات المختلفة التي يمكن أن يتمتع بها أي تطبيق حصان طروادة. ومن المحتمل أن تصبح عائلة تطبيقات حصان طروادة Optix الشائعة منافساً رئيسياً للتطبيق Sub7. هذه التطبيقات مجانية، لكن مطورو التطبيق Optix والتطبيقات الأخرى من شركة EES يقدمون خدمات برمجة تطبيق حصان طروادة غير قابل للكشف للزبائن بسعر 300 دولار أمريكي. ويمكنك الحصول على التطبيق Optix وغيره على الرابط www.evileyesoftware.com.

NET-DEVIL: تطبيق حصان طروادة شائع جداً، كامل المواصفات، يستطيع تدمير جدار حماية وبرنامج مكافحة الفيروسات في حالة التشغيل. يتميز بثباته العالي وخاصة في نظام التشغيل Windows XP. توقف مطور التطبيق Nilez عن تحديثه في بداية عام 2003. يعتبر Net-Devil أداة تجسس جيدة ويتوفر على الرابط www.net-devil.com/main.html.



الشكل (2-9) عميل تطبيق حصان طروادة Optix Pro، يظهر الأوامر التي يمكن إرسالها إلى ملقم بعيد، بما فيها استخلاص كلمات مرور مخزنة.

أساليب: ما داخل عقل محارب طروادة

إذا كنت راغباً باستخدام تطبيقات حصان طروادة كجزء من أدواتك التجسسية، أنصحك بأن تقضي بعض الوقت لتتعلم وتتعرف على ثقافة مستخدمي ومطوري تطبيقات حصان طروادة.

من أحد أشهر الأماكن التي تجمع مستخدمي ومطوري تطبيقات حصان طروادة هو الموقع TrojanForge (www.trojanforge.net). يُظهر هذا الموقع منتدى حيث يقوم الأعضاء بتبادل أية معلومات حول تطبيقات حصان طروادة وبرامج مكافحتها. كما يوجد أيضاً قسم للنشر، حيث يقوم مطورو تطبيقات حصان طروادة بالإعلان عن منتجاتهم والحصول على آراء المطورين والمستخدمين.

كما يمكننا الإشارة إلى أنه من أحد زوار الموقع TrojanForge أو غيره، هم بائعو منتجات مكافحة الفيروسات وتطبيقات حصان طروادة، حيث يقوم هؤلاء بتفقد مثل هذه المواقع بصورة دورية لمعرفة المستوى الذي وصل إليه خصومهم. كما أنه من غير البعيد قيام وكالات الاستخبارات بزيارة مثل هذه المواقع لكونها مهتمة باستخدام تطبيقات حصان طروادة لأغراض تجسسية، وذلك ليبقوا على إطلاع حول التقنيات الجديدة التي يمكن أن يستخدموها أو يدافعوا عن أنفسهم بها. لكن بالتأكيد لن ترى رسالة من وكالة الاستخبارات المركزية CIA في قسم النشر وهي تعلن عن تطبيق حصان طروادة جديد والذي يعمل على أنظمة كوريا الشمالية العتيقة.

يتضمن كل موقع لتطبيقات حصان طروادة تقريباً عدة تطبيقات يمكنك تحميلها، لكن هناك بعض المواقع المتخصصة بتطبيقات حصان طروادة أكثر من غيرها، ومن بينها المواقع التالية:

- **Evil Eye Software**: موقع تحميل ومنتدى لفريق تطوير تطبيقات حصان طروادة لصالح الموقع (www.evileyesoftware.com).
- **Fearless**: منتدى جمع وتحميل لفريق تطوير تطبيقات حصان طروادة للموقع (www.areyoufearless.com).
- **SinRed**: أخبار وملفات من فريق تطوير تطبيقات حصان طروادة للموقع (www.sinred.com).
- **MegaSecurity**: موقع عام لأمن الحواسب ومتخصص بتطبيقات حصان طروادة (www.megasecurity.org/Main.html).

إذا كنت تخطط لاختبار تطبيقات حصان طروادة لأغراض تجسسية من أي من المواقع السابقة أو غيرها من المواقع السرية، يجب أن تتحصن بجميع أنواع برامج الحماية (جدران الحماية، ترميمات حديثة للمستعرض، وبرمجيات مكافحة الفيروسات وتطبيقات حصان طروادة). وإذا كنت قلقاً بشأن مراقبة أحد ما لاستعراض الإنترنت، فقد ترغب أيضاً باستعمال بعض الأدوات المجهولة التي سوف تمر معنا في الفصل العاشر.

المنتجات التجارية

سوف تصادف، في كل مكان طوال هذا الكتاب، أمثلة عن منتجات تجارية مصممة بشكل أساسي لإدارة النظام، والتي يمكن استخدامها أيضاً لأغراض شريرة. هناك عدد من المنتجات التي تستخدم للإدارة البعيدة للحواسب والتي تتمتع بنفس إمكانيات تطبيقات حصان طروادة ذات الوصول البعيد (باستثناء عدم وجود بعض الحيل الطريفة مثل فتح وإغلاق محرك الأقراص المضغوطة باستمرار). وبما أن هذه التطبيقات شرعية، فبالتالي لن تكشفها برمجيات مكافحة الفيروسات وتطبيقات حصان طروادة، إذا تم تثبيتها سرياً على الحاسب.

كما يمكن الاستفادة من أمر وهو أن تطبيقات الإدارة البعيدة قد تكون مثبتة مسبقاً على الحاسب الهدف، مما يسّهل مهمتك (ما عليك إلا استعمال نسختك من الأداة للوصول إلى الحاسب البعيد). تستخدم التطبيقات التجارية أيضا، مثل تطبيقات حصان طروادة، منافذ ثابتة أو افتراضية (اتبع الرابط www.iana.org/assignments/port-numbers للحصول على قائمة المنافذ المسجلة والتطبيقات والبروتوكولات التي تستخدمها)، فعلى سبيل المثال، يشير المنفذ 5631 المفتوح إلى عمل التطبيق الشهير pcAnywhere. لكن ظهر عدد من المساوئ لعدد من المنتجات الإدارية، وإذا كان هدفك يستخدم أحدها فمن الجدير أن تجري بحثاً عنها. بالإضافة إلى ذلك، يوجد عدد من البرامج الخدمية المتوفرة والتي تقوم بمهاجمات القاموس على التطبيقات التجارية والتي تملك اتصالات محمية بكلمة مرور.

هناك تطبيقان شائعان للإدارة البعيدة وهما:

- **pcAnywhere**: منتج من شركة Symantec. وهو أداة شائعة جداً للتحكم بالحواسب عن بعد عبر شبكة أو اتصال هاتفي. يتميز التطبيق بعدد من الخصائص لمقاومة المتلصصين، لكن إذا استطاع الجاسوس الوصول الفيزيائي إلى الحاسب واستطاع تثبيت التطبيق، فهو فعال مثل أي تطبيق حصان طروادة. تتوفر معلومات حول تطبيق pcAnywhere على الرابط /www.symantec.com/pcanywhere.
- **VNC**: وهو عبارة عن حزمة برمجية مجانية، مفتوحة المصدر، متعددة المنصات عميل/ملقم، وهي اختصار للعبارة Virtual Network Computing. وتقوم هذه الحزمة البرمجية بتزويد وصول بعيد عبر الشبكة إلى سطح المكتب الرسومي.

تستطيع من خلال حزمة VNC الوصول إلى الحاسب من أي مكان عبر الاتصال بالإنترنت. يمكن تحميل هذه الحزمة من موقع مختبرات AT&T لجامعة Cambridge، على الرابط www.uk.research.att.com/vnc/. تتوفر أيضاً نسخة مطوّرة من حزمة VNC (مفتوحة المصدر أيضاً)، وتسمى TightVNC، ويفضّلها الكثير من مدراء الأنظمة بسبب أدائها وأمنها المتميز. يمكنك تحميلها من خلال الرابط www.tightvnc.com.

والآن عودة إلى قصتنا المشوقة. بعد أن قام أخوك بغسل دماغك بقصصه حول أحصنة طروادة، قررت أن ترسل رسالة إلكترونية إلى المغنية مستخدماً برنامج Optix Lite تقوم بإرفاق ملف يتضمن تطبيق حصان طروادة (طبعاً، من بريد إلكتروني مزيف ومن مقهى إنترنت). خطتك هي استخدام تطبيق حصان طروادة صغير للحصول على موطئ قدم إلى حاسبها ومن ثم تقوم بإيداع النسخة Optix Pro لزيادة المراقبة على نشاطاتها. تستخدم مهاراتك في الكتابة لتحرير رسالة شخصية من صديق تعرف أنها ستفتحه. أنت واثق من أن هذا التجسس الإلكتروني سيمنحك فرصة أخرى لتستعيد عملك الصحفي.

الإجراءات المضادة

والآن سوف نعود إلى دور الخير، أنت تعمل في خدمة الحماية التنفيذية، وقد قامت مغنية مشهورة باستخدامك لتقوم بحمايتها وحماية مصالحها. هناك فريق من الخدمة بالغة السرية وعملاء مكتب التحقيقات الفدرالي والذين يقومون بالحراسة الشخصية الفعلية، أما مهمتك فتتلخص في معالجة قضايا الأمن الحاسبي وبشكل خاص تعقب أثر الجواسيس الإلكترونيين.

تمر جميع رسائل البريد الإلكتروني الواردة عبر برنامج ترشيح مخصص قمت ببرمجته لفحص الملفات المرفقة برسائل البريد الإلكتروني ضد الفيروسات. البريد الإلكتروني الشخصي للمغنية غير معروف، لكنك تلتقط أحياناً بعض الرسائل العرضية من الغرباء والتي تحمل الفيروس SirCam والتي من المحتمل أن تكون قد أتت من دفتر العناوين الخاص بمعارفها الشخصية. في أحد الأيام، وجدت أمراً غريباً عندما قمت بالتحقق من السجلات. رسالة إلكترونية حيث لا تتطابق فيها ترويسة "من From" مع ترويسة "الاستقبال Received" (والتي لم تُعرض فعلياً)، من الواضح أن هذه رسالة انتحال مرسلة من أحد أصدقائها (لمزيد من المعلومات حول رسائل الانتحال، اتبع الرابط (www.stopspam.org/email/headers/headers.html. ومن المثير للاهتمام أن هناك ملف مرفق لا يتضمن فيروس، بل يتضمن تطبيق حصان طروادة صغير.

تبدو هذه الرسالة الإلكترونية معقدة جداً لتكون من أعمال الأطفال الأشقياء، وتقلق أنك تواجه جاسوساً إلكترونياً خطيراً. بعد أن تطلع رئيسك تقرران أن تدعا تطبيق حصان طروادة يعمل على حاسب مراقَب بشدة، وإذا حاول أحد ما الاتصال بالتطبيق ستقوم باقتفاء أثره. بعد عدة أيام يقوم أحد ما بتفعيل التطبيق، وتبدأ بتسجيل جميع النشاطات وتحديد عنوان IP للاتصال القادم.

بعد مرور عدة أيام من تنصت الجاسوس على رسائل إلكترونية مزيفة، وتحميل ملفات غير حقيقية قمت بزرعها على الحاسب، يقرر رئيسك أن الوقت حان لإيقاف هذه العملية ويتصّل

بعض أصدقاءه في وزارة العدل (في النهاية، هذا الهجوم انتهاك واضح لعدد من القوانين الفدرالية المتعلقة بالتنصت والجريمة الحاسبية). تقوم بتسليم جميع المعلومات والسجلات التي جمعتها إلى عميل يعمل لصالح مكتب التحقيقات الفدرالي، وبعد مرور أسبوع تقرأ في جريدة مقالة عن اعتقال هاوٍ مجنون في مقهى إنترنت أثناء قيامه بتحميل رسالة إلكترونية لمغنية مشهورة بعد أن قام باقتحام حاسبها.

بالرغم من أن تطبيقات حصان طروادة قد تكون ماكرة جداً، في الحقيقة يوجد هناك عدد من الإجراءات المضادة التي يمكن أن تطبقها لتحمي نفسك نسبياً من أن تقع ضحية عمل تجسسي. سوف نغطي في الفقرات التالية بعض إجراءات الحماية.

دفاعات الشبكة

يوجد عدد من إجراءات الحماية الشبكية لاكتشاف تطبيقات حصان طروادة ذات الوصول البعيد والتغلب عليها، ومن ضمنها ما يلي:

- **استعراض اتصالات الشبكة:** يستخدم ملقم تطبيق حصان طروادة منفذاً ما للاتصال بالعميل. إذا فحصت المنافذ المفتوحة ووجدت منفذاً أو أكثر غير مرتبط بنظام التشغيل Windows أو أي تطبيق معروف، فقد يكون لديك دليل وجود تطبيق حصان طروادة.
- **استخدام جدار الحماية:** يستطيع جدار الحماية الذي يعرقل الاتصالات الشبكية الخارجة إيقاف تطبيق حصان طروادة عند محاولته الاتصال بالإنترنت. لكن عليك توخ الحذر، حيث تتمتع تطبيقات حصان طروادة الحديثة بالقدرة على اختراق تطبيقات جدار الحماية (عدّل بعض بائعي تطبيقات جدار الحماية منتجاتهم لجعل عملية اختراقها أكثر صعوبة). يجب أن تتحقق دورياً من وجود أيقونة تطبيق جدار الحماية ضمن شريط المهام في النظام Windows، ومع ذلك يستطيع تطبيق حصان طروادة ماكر للغاية أن يضيف ببساطة أيقونة مزيفة لتطبيق جدار الحماية إلى شريط المهام بعد إيقاف عمل التطبيق، لإيهام المستخدم أن التطبيق لا يزال يعمل.
- **مراقبة حركة المرور للشبكة:** تستطيع مراقبة حركة المرور للشبكة المتولدة والواصلة إلى حاسبك، باستخدام برنامج sniffer (محلّل شبكي). حيث تمثّل حركة المرور الغريبة، المنافذ غير القياسية، وعناوين IP مجهولة إشارات تحذيرية عن احتمال تثبيت وتشغيل تطبيق حصان طروادة. تشفّر بعض تطبيقات حصان طروادة بياناتها، لذلك إذا صادفت بيانات غير اعتيادية والتي تبدو ممزوجة أو لا تتطابق مع بروتوكول معروف، فقد تكون إشارة تحذيرية أيضاً.

تتم مناقشة هذه الإجراءات الدفاعية، والتي تعمل بصورة جيدة لأنواع المهاجمات الشبكية الأخرى، بالتفصيل الممل في فقرة "الإجراءات المضادة" من الفصل العاشر.

استخدام برامج مراقبة التسجيل ومدققات تكامل الملفات

لتستطيع تطبيقات حصان طروادة العمل في كل تشغيل للنظام Windows، تقوم عادة بتعديل التسجيل، إضافة ملف إلى مجلد بدء التشغيل، أو تعديل أحد ملفات الأوامر لبدء التشغيل مثل AUTOEXEC.BAT أو WIN.INI على الأنظمة الأقدم.

يمكن كشف هذه التعديلات باستخدام برامج مراقبة التسجيل ومدققات تكامل الملفات. يقوم برنامج مراقبة التسجيل بإعلامك عند إضافة أو تعديل مفاتيح التسجيل، أما برامج تدقيق تكامل الملفات تعمل عن طريق الانتقال عبر الأدلة وحساب قيم التجزئة (مثل القيمة MD5) لكل ملف. بعد حصول مدقق تكامل الملفات على هذه المعلومات الأساسية، عندما يتم تنفيذ الأداة مرة أخرى، تقوم بإعادة حساب قيم التجزئة للملفات وتقارنها مع القيم الأصلية. إذا لم تتطابق هذه القيم فسوف تعلم أنه تم تعديل الملف وإذا كان هذا الملف تطبيق أو ملف نظام فقد يكون هذا نتيجة تطبيق حصان طروادة. سوف يحميك استخدام هذه الأدوات ضد تطبيقات حصان طروادة الجديدة والتي قد لا تكشفها برامج المكافحة.

توجد أداتان مجانيتان شائعتان لكشف التغييرات الطارئة على التسجيل والملفات وهما:

- **RegistryProt**: أداة شائعة لشركة CSDiamond وتقوم بتحذيرك في كل مرة يتم فيها إضافة أو تعديل قيمة مفتاح التسجيل. تتوفر هذه الأداة على الرابط:
www.diamondcs.com.au/web/htm/regprot.htm.
- **مراقب تكامل النظام GFI LANguard**: تفحص هذه الأداة فيما إذا تم تغيير، إضافة، أو حذف الملفات على أنظمة التشغيل Windows 2000/XP. يمكنك تحميل الأداة من الرابط: www.gfi.com/lansim/index.html.



لمزيد من برامج مراقبة التسجيل ومدققات تكامل الملفات والتي تستطيع اعتراض تطبيقات حصان طروادة، قم بالإطلاع على قائمة الأدوات الأمنية المجانية على الرابط www.wilders.org/free_tools.htm.

استخدام برمجيات مكافحة الفيروسات

تتضمن معظم الحزم البرمجية لمكافحة الفيروسات تطبيقات حصان طروادة الشائعة الاستخدام فقط ضمن قواعد بياناتها. يركّز البائعون بشكل أساسي على الفيروسات، أما تطبيقات حصان طروادة فهي غالباً في المرتبة الثانية. من أحد منتجات مكافحة الفيروسات التي تتلقى احتراماً كبيراً من قبل مطوري ومستخدمي تطبيقات حصان طروادة، المنتج Kaspersky Anti-Virus (KAV)، والذي يتمتع بسمعة ممتازة لكشف الفيروسات إلى جانب تطبيقات حصان طروادة. لمزيد من المعلومات عن المنتج KAV، اتبع الرابط www.kaspersky.com.

استخدام برمجيات كشف تطبيقات حصان طروادة

لضمان الحماية الكاملة ضد تطبيقات حصان طروادة، إضافة لتنفيذ برمجيات مكافحة الفيروسات، يجب أن تستخدم برمجيات كشف وإزالة تطبيقات حصان طروادة. مع أن هذه البرمجيات غير واسعة الانتشار مثل برمجيات مكافحة الفيروسات، إلا أن بائعي هذه المنتجات يلقون كامل الاهتمام على تطبيقات حصان طروادة ليحافظوا على أحدث الإصدارات والمعلومات السرية. لا يتوقع معظم مستخدمي تطبيقات حصان طروادة أن ضحاياهم يقومون بتشغيل برمجيات لكشف هذه التطبيقات، مما يؤدي إلى إحباط جميع مخططاتهم.

من المهم أن تعلم أن برمجيات كشف تطبيقات حصان طروادة سوف تكشف التطبيقات المعروفة فقط والمخزنة ضمن قاعدة بيانات المنتج (كما يجب أن تحرص على تحديث هذه البرمجيات بشكل مستمر كما هي الحالة في برمجيات مكافحة الفيروسات). أما تطبيق حصان طروادة غير المعروف والذي تمت برمجته بشكل خاص قد لا يتم كشفه. إذا كنت تشك بأنك هدف محتمل لحملة تجسسية معقدة، قم باستخدام سلسلة دفاعات متعددة الطبقات لتحسين الأمن لديك.

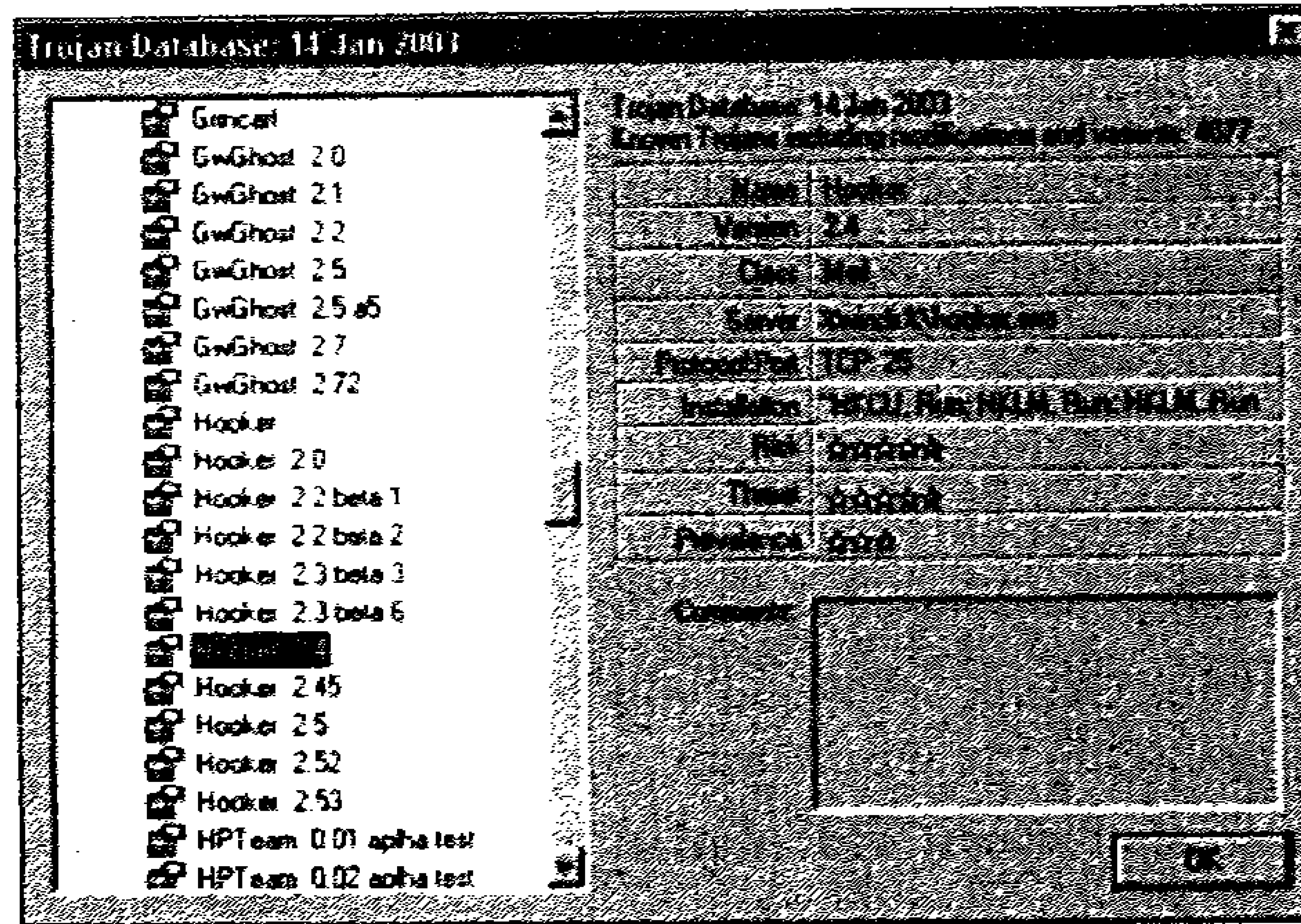
يوجد عدد من المنتجات في الأسواق والتي تزعم أن بمقدورها كشف وتدمير أية تطبيقات حصان طروادة موجودة أو التي تحاول أن تثبت. تتنوع نسبة الكشف بين هذه المنتجات، اعتماداً على نوع المراجعات التي تقرأها، لكن هناك حفنة من المنتجات والتي تظهر نموذجياً في اللوائح المفضلة وهي:

- **Trojan Defense Suite (TDS)**: سعرها 49 دولاراً أمريكياً، مع توفر إصدار تجريبي على الرابط /http://tds.diamondcs.com.au.

- **BOClean**. سعرها 39.95 دولاراً أمريكياً على الرابط www.nsclean.com/boclean.html.
- **Tauscan**، 29.95 دولاراً أمريكياً، مع توفر إصدار تجريبي على الرابط www.agnitum.com/products/tauscan/. (انظر الشكل 3-9).
- **Trojan Hunter**، 34.95 دولاراً أمريكياً، مع توفر إصدار تجريبي على الرابط www.misec.net/trojanhunter.



أصدرت شركة Mischel Internet Security مؤخراً، مطور الأداة Trojan Hunter، برنامج محاكاة مجاني لتطبيق حصان طروادة والذي يمكن أن تستخدمه بأمان لتختبر تطبيقات حصان طروادة والتطبيقات الأمنية الأخرى، يتوفر على الرابط www.misec.net/trojansimulator.



الشكل (3-9) برنامج الفحص Tauscan يُظهر تطبيق حصان طروادة مسجل مفاتيح مع شرح عن البرنامج الخبيث المكتشف (البرامج الخبيثة malware: مصطلح عام يشير إلى تطبيقات حصان طروادة، الفيروسات، برامج الدودة، والبرمجيات الخبيثة الأخرى).

إزالة تطبيقات حصان طروادة

تزيل برمجيات كشف تطبيقات حصان طروادة التطبيقات التي تكشفها آلياً، لكن بالرغم من ذلك يجب أن تنسخ بياناتك الهامة إلى قرص مضغوط، تعيد تهيئة القرص الصلب للحاسب المصاب، وتعيد تثبيت نظام التشغيل Windows. قد تبدو لك هذه العملية شديدة، لكن لا يمكن

أن تتوقع ما قد يكون فعل تطبيق حصان طروادة للنظام أثناء عمله، ومن الأفضل أن تكون آمناً وليس نادماً. (قد تكون ملفات البيانات أصيبت بفيروس الماكرو، لذلك تأكد من تشغيل برنامج لمكافحة الفيروسات قبل أن تسترجع الملفات إلى النظام الجديد).

توجد عدة طرق لإزالة تطبيق حصان طروادة يدوياً من نظامك. أولاً يجب أن تحدد مع من تتعامل يتم ذلك عادة بتعقب المنفذ المفتوح إلى التطبيق المطلوب. أجر بحثاً عن طريق محرك البحث Google عن اسم تطبيق حصان طروادة لتتزود بالمعلومات المناسبة عنه. تحوي الكثير من مواقع مكافحة الفيروسات أوصافاً لتطبيقات حصان طروادة الشائعة مع تعليمات إزالتها. إذا استطعت إيجاد نسخة من عميل التطبيق و لم يكن الملقم محمياً بكلمة مرور، قد تستطيع إزالة الملقم لأن معظم برامج العميل تستطيع إلغاء تثبيت وإزالة الملقم. انسخ العميل إلى الحاسب المصاب، ومن ثم قم باختيار 127.0.0.1 (مضيف محلي) لعنوان IP وحاول الاتصال بالملقم.

استخدام برمجيات من شركات أخرى غير شركة Microsoft

بما أن تطبيقات شركة Microsoft، مثل Microsoft Internet Explorer وOutlook/Outlook Express، حافلة بتاريخ مليء بالأخطاء والثغرات، يفضل أن تقوم باستبدال برنامج المستعرض وعميل البريد الإلكتروني بتطبيقات من طرف ثالث. مع أن شركة Microsoft تستمر بترميم منتجاها عند ظهور الثغرات والأخطاء، يزيد العدد الكبير لنقاط الضعف حالياً (واحتمال وجود نقاط ضعف غير مصرح بها) من تعرضك إلى مهاجمات شبكية ناجحة.

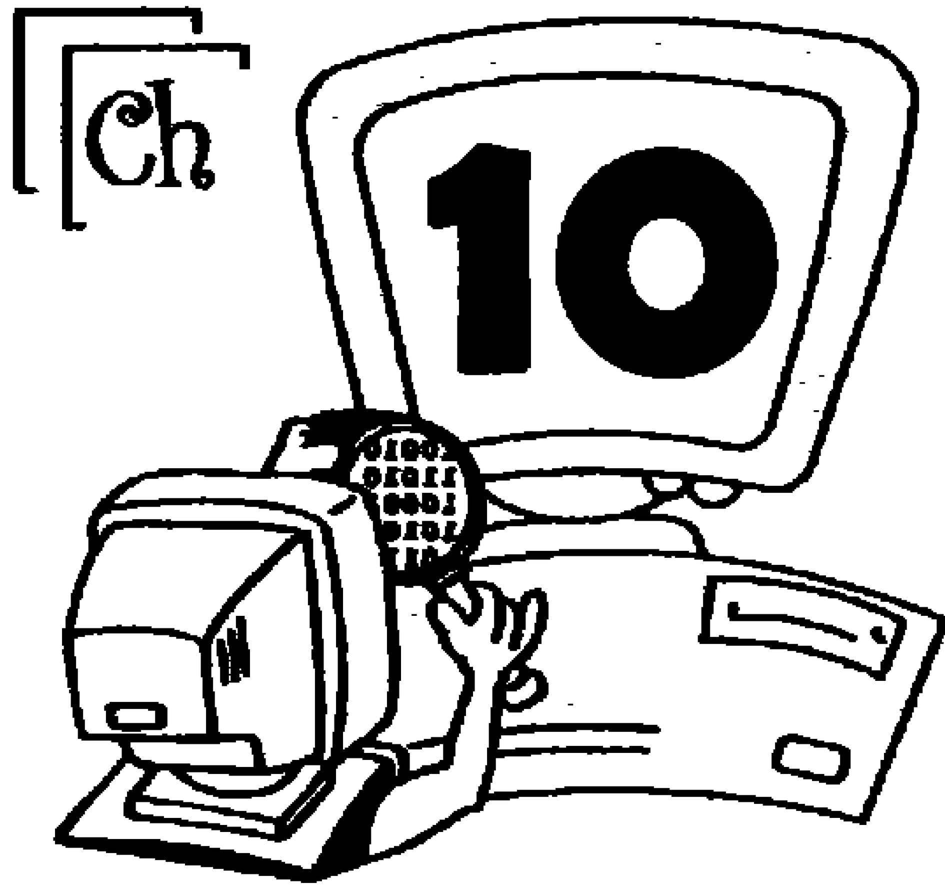
تلخيص

تطبيقات حصان طروادة أدوات فعالة جداً في عمليات التجسس الحاسبية، وخاصة ضد الأهداف الساذجة وغير المستعدة. تستخدم تطبيقات حصان طروادة الشبكية في هجومها الملفات المرفقة بالبريد الإلكتروني. صفحات الويب، أو التطبيقات المعدلة التي يتم تحميلها من الشبكة. تمنح الوسائل السابقة الجاسوس موطئ قدم إلى حاسب الضحية حتى على بعد آلاف الأميال. أما إذا كان لديك وصول فيزيائي للحاسب، من الأسهل استخدام تطبيق حصان طروادة لأنه غالباً يمكنك تجاوز الإجراءات الأمنية لتثبيت طريقة ملتوية للدخول.

حتى الآن يجب أن تتم برمجة تطبيق حصان طروادة الذي لا يمكن قهره، لكن حتى تحين تلك اللحظة قم باستخدام الإجراءات المضادة التي عرضناها من خلال هذا الفصل ويجب أن تكون قادراً على كشف وإزالة أي من تطبيقات حصان طروادة الحالية.

التقنية الجديدة لتطبيقات حصان طروادة تتقدم بسرعة كبيرة، مع وجود المطورين لتطبيقات حصان طروادة والبائعين لبرمجيات مكافحتها الذين يتنافسون ضد بعضهم. لا تزود المصادر الأمنية الأساسية تغطية كبيرة للتطورات الجديدة على ساحة تطبيقات حصان طروادة، ويجب أن تراقب بعض المواقع السرية التي تبقى مواكبة للتهديدات الجديدة.

وتذكر دائماً، احذر اليونان الحاملين للهدايا.



التنصت على الشبكة

مقدمة إلى التجسس على الشبكات

إذا لم تحقق الوصول الفيزيائي إلى الحاسب، فإنك تستطيع دوماً أن تتنصت عليه إذا كان متصلاً بشبكة. لقد جعلت شعبية شبكة الإنترنت عشرات الملايين من الحواسب معرّضة للمهاجمات الشبكية المحتملة. عندما تقول "مهاجمة شبكية Network Attack"، فأول شيء يخطر على أذهان الناس هو المخرّب الماكر الذي يحاول اختراق الحاسب، التجسس الشبكي قريب جداً إلى التخريب لأن الجاسوس يستخدم الكثير من الأدوات والتقنيات المشابهة لما يستخدمه المخرّب أثناء اختراقه للنظام. يكمن الفرق الأساسي بين المفهومين أن عملية التجسس المنفذة احترافياً سوف تكون أصعب بكثير أن تكشف من المهاجمة الشبكية اليومية الشائعة، والتي تخلّف غالباً كثيراً من الإشارات الواضحة.

يقدم هذا الفصل نظرة عامة للتجسس على الشبكات السلكية (ستتم مناقشة التنصت على الشبكات اللاسلكية في الفصل الحادي عشر)، بما فيها استخدام برامج sniffer، الماسحات غير المحصّنة، وأدوات أخرى قد يستعيرها الجاسوس من حقيبة أدوات المخرّب. كما سنناقش عدداً من الإجراءات المضادة المقاومة لكثير من هذه المهاجمات.

بما أنه يتم تكريس كتب كاملة للمهاجمات الشبكية، فإن الهدف من هذا الفصل هو إعطائك معرفة عملية أساسية لتفاصيل التنصت الشبكي. وإذا كنت مهتماً بتطوير وصقل مهاراتك في التجسس الشبكي، فهناك عدد من المراجع في مواقع ويب ومصادر أخرى تتيح تفاصيل أكثر حول نقاط الضعف التي يمكن استغلالها. قبل أن ندخل ضمن بعض الأساليب المعينة التي يستخدمها الجواسيس لاختراق الحواسب على الشبكة، من الجدير أن نذكر بعض المفاهيم العامة للتجسس الشبكي.

أنواع المهاجمات الشبكية

بالرغم من وجود آلاف المهاجمات الشبكية المحتملة المبنية على أنواع مختلفة من نقاط الضعف، عموماً، يمكن أن يتم كشف البيانات بطريقتين مختلفتين.

- **هجوم سلبي Passive attack**: المهاجمات السلبية هي محاولات لكشف المعلومات عن طريق مراقبة حزم البيانات المارة عبر الشبكة وتتضمن غالباً استخدام أحد أنواع البرامج لمراقبة الشبكة (sniffer) للتنصت على الحاسب واستعراض البيانات. بالرغم من أنه يمكن نظرياً كشف برنامج sniffer، إلا أنه من الصعب جداً كشف هذا النوع من الهجوم.
- **الهجوم النشط Active attack**: تكشف المهاجمات النشطة البيانات على القرص الصلب أو وسائط التخزين الأخرى مباشرة وذلك بالاستفادة من الثغرات المتواجدة في نظام التشغيل والتطبيق أو التدريبات الأمنية السيئة. مثلاً، سرقة المستندات من نظام حيث تم تفعيل مشاركة الملفات عبر الشبكة، لكن لم يتم تعيين كلمة مرور للحد من الوصول إلى الملفات المشاركة. مثال آخر هو تطبيق حصان طروادة يقوم بإرسال بيانات الجاسوس سرياً عبر الاتصال الشبكي. تمت مناقشة هذا النوع من المهاجمات في الفصل التاسع.

إضافة إلى المهاجمات السلبية والنشطة، توجد أيضاً مهاجمات مستهدفة وعشوائية:

- **الهجوم المستهدف Targeted attack**: يقع الهجوم المستهدف عندما يتم اختيار حاسب محدد أو مجموعة من الحواسب لشن الهجوم. فإنه يمكن أن يتم شن الهجوم عن بعد ضد عناوين IP معروفة أو ضد الشبكة نفسها وذلك عن طريق اختراق الأمن الفيزيائي وتثبيت جهاز تنصت على الشبكة. أما إذا تم شن الهجوم من خارج الشبكة، يمكن الحصول على معلومات الاستهداف القيّمة من أدوات مرتبطة بملقم اسم المجال DNS، مثل الخدمات whois، dig، أو tracert. مع هذا النوع من الهجوم تمّ اختيارك بشكل خاص لسبب محدد، فإذا كانت هذه هي الحالة، قد لا تكون الإجراءات المضادة البسيطة كافية لإيقاف المتطفل المصمم.
- **الهجوم العشوائي Random attack**: في هذا النوع من المهاجمات، الأكثر شيوعاً، السبب الوحيد لتعرضك للهجوم هو أن أحداً ما عثر على عنوان IP الخاص بحاسبك بالصدفة خلال مسح الأنظمة المعرضة للهجوم. يتم شن المهاجمات العشوائية غالباً من قبل المخربين الباحثين عن حاسب للاختراق لاستخدامه كنقطة وصل للمهاجمات الأخرى، لتخزين الملفات غير الشرعية عليه، لشن مهاجمات لتعطيل الخدمة (Denial of Service attacks) باستخدامه، لتنفيذ ملقمات خدمة التحادث عبر الإنترنت IRC، أو فقط لتكون ماكراً. هذه المهاجمات بالمصادفة هي عمل المخربين أو المجرمين الانتهازيين لكن ليس الجواسيس، لكن حتى لو لم يسعى المتطفل يسعى خصيصاً للحصول على بياناتك إلا أنها سوف تتعرض للكشف إذا تم اختراق نظامك.

مصادر المهاجمات الشبكية

على خلاف المهاجمات المعتمدة على الوصول الفيزيائي للحاسب، يمكن شن محاولات التنصت على الشبكة من عدد من المواقع المختلفة. يستفيد الجاسوس من هذه العملية في أمور عدة ومن بينها صعوبة التقاطه وكشفه. إذا تم تنفيذ الهجوم بصورة صحيحة، فإن كشف محاولة اختراق النظام عبر الشبكة والتحقيق فيها أصعب من عمل الحقيبة السوداء، وأقل خطراً بكثير.

فيما يلي بعض المواقع التي يمكن البدء بالهجوم منها:

- **المقبس الجداري أو السلك الشبكي:** من الواضح أن هذا الهجوم يتطلب وصولاً فيزيائياً إلى البناء حيث يتم استعمال الشبكة. يتصل الجاسوس بالشبكة عبر اتصال غير مستخدم في مكان ما ضمن البناء (أو يتنصت على السلك). تعتبر الحواسب المحمولة Laptops وأجهزة المساعد الرقمي الشخصي PDAs أدوات مثالية لهذا النوع من الهجوم بسبب حجمها الصغير. كما يمكن أن يقوم الفريق التقني بلصق تسمية على كبل شبكة Ethernet أو المقبس الجداري تتضمن عنوان IP الخاص بها، لتسهيل إدخاله ضمن إعدادات الشبكة. أما إذا استعمل الملقم بروتوكول التكوين الديناميكي للمضيف DHCP (Dynamic Host Configuration Protocol)، فسوف يتم إسناد عنوان IP آلياً إلى حاسب الجاسوس إذا تم تكوينه ليقبل عنواناً ديناميكياً. أي التجسس على شبكة ركّب ثم شغّل. لكن يجب إجراء بعض البحث سابقاً لكشف أسماء المجال وحسابات المستخدم للمهاجمات المستهدفة.
- **حاسب عميل في الشبكة:** وهنا يعتمد الجاسوس على حاسب موجود مسبقاً في الشبكة. مع أنه قد يتم استهداف المعلومات الموجودة على القرص الصلب، إلا أن الهدف الأكبر هو الوصول إلى بقية الحواسب على الشبكة وكشف المعلومات المخزنة داخلها. قد يكون هذا النوع من الهجوم مدمراً جداً لأن معظم المواقع تتمتع بإجراءات الدفاع التي تحمي الشبكة من الهجوم الخارجي، لكن تبقى الأمور مفتوحة للمهاجمات الداخلية.
- **ملقم داخل الشبكة:** يمنح الوصول الفيزيائي للملقم خيارات تنصت متعددة للجاسوس. يمكن استخدام الملقم كنقطة انطلاق لاختراق بقية الحواسب، قراءة ومراقبة تسجيلات الملقم، تثبيت برنامج sniffer، وأخيراً كشف البيانات المخزنة. تتمتع الملقمات عادة بإجراءات فيزيائية أمنية إضافية لحمايتها، لكنها قد لا تكون فعالة لردع جاسوس محترف.
- **حاسب من خارج الشبكة:** هذا هجوم تقليدي من قبل المخرّب، حيث يقوم الجاسوس بشن الهجوم على حواسب من ضمن الشبكة (إما عميل client أو ملقم server) من حاسب خارج الشبكة. يقضي معظم مدراء النظام وقتاً طويلاً ويبذلون جهداً كبيراً محاولين ردع هذا النوع من الهجوم. يقوم الجاسوس الذكي بشن الهجوم من خلال سلسلة من

الحواسب لإخفاء أثره. فعلى سبيل المثال بدلاً من أن يستخدم حساب الإنترنت الخاص به، يقوم الجاسوس بزيارة مقهى إنترنت ويتصل أولاً بحاسب متوضع في رومانيا عن طريق خدمة الاتصال عن بعد telnet، ومن ثم بنفس الطريقة يتصل بحاسب متوضع في اليابان، وأخيراً يتصل بالحاسب المستهدف في جامعة مكسيكو ليبدأ هجومه من هناك. وفي حال استطاع أحدهم اقتفاء أثره عن طريق عناوين IP عبر المسار العالمي، فسوف يصل إلى طريق مسدود عندما يكتشف أن هذه المهاجمات بدأت من مقهى الانترنت.

المعلومات المعرضة للكشف أثناء الهجوم الشبكي

دعونا نوضح معنى القول "المعلومات المعرضة للكشف" أثناء الهجوم الشبكي، ولندخل في تفاصيل نوعية البيانات التي يمكن أن تكشف أثناء التنصت على الشبكة. تحدثنا في الفصل الخامس عن نوع المعلومات والأدلة التي يمكن استخلاصها من القرص الصلب إذا تمكن الجاسوس من الوصول الفيزيائي إلى الحاسب، وبالتالي يجب أن تعرف ما هي أنواع المعلومات والأدلة التي يمكن جمعها خلال الهجوم الشبكي.

تتضمن بعض المعلومات التي يمكن أن تكشفها، إذا كنت جاسوساً، أو التي يمكن أن تحميها إذا كنت تحاول تأمين النظام، ما يلي:

- **البريد الإلكتروني:** إلى من ترسل الرسالة الإلكترونية، ممن تستقبلها، متى ترسلها وتستقبلها، وما هو محتواها (من بينها الملفات المرفقة) جميع هذه المعلومات تمر عبر الشبكة.
- **كلمات المرور:** يمكن التنصت بسهولة على أسماء الحسابات وكلمات المرور التي يتم إرسالها بتنسيق صريح (غير مشفر) عبر الشبكة، ومن ضمنها كلمات المرور الخاصة بالبريد الإلكتروني، بروتوكول FTP، والاتصال عن بعد Telnet، ومعلومات تسجيل الدخول إلى موقع ويب (إذا لم يستخدم الموقع طبقة المقابس الآمنة لتشفير البيانات).
- **جلسات المراسلة الفورية والدردشة:** يمكن اعتراض كلا جانبي المحادثة خلال جلسات المراسلة الفورية أو الدردشة إذا لم تكن مشفرة.
- **الاتصالات الصوتية والمرئية:** يمكن مراقبة أية اتصالات مرئية أو صوتية غير مشفرة (مثل الأصوات عبر الإنترنت أو البروتوكولات الأخرى).
- **عادات تصفح صفحات الإنترنت:** يمكن أن يتم توليد مظاهر سلوكية عنك وذلك عن طريق تفحص أنواع مواقع الويب التي تقوم بزيارتها ونشاطاتك ضمن الموقع (متى تقوم بالزيارة، عما تبحث، وتردد زياراتك).

- **مناقلات تبادل الملفات:** يمكن مراقبة عمليات إيداع الملفات، تحميلها، أو عمليات البحث على شبكات الند للند.
- **بيانات القرص الصلب:** يستطيع الجاسوس شن هجوم نشط على حاسبك من خلال اتصال شبكي لتجميع المعلومات من الملفات أو المجلدات المشتركة. كما يمكنه أيضاً استخدام هجوم باستخدام تطبيق حصان طروادة، كما مر معنا في الفصل التاسع، ليملك تحكماً كاملاً عن بعد على حاسبك.

أخطار النطاق العريض

لقد زادت عملية اتخاذ الوصول إلى الإنترنت ذات النطاق العريض من خلال خط المشترك الرقمي DSL (Digital Subscriber Line) وأجهزة المودم الكبلية (Cable Modems)، احتمالات التجسس الحاسبي. مع أن الشبكات المشتركة والحكومية تكون محمية ضد المهاجمات الشبكية، إلا أن معظم الأنظمة المترلية لا تتمتع بنفس مستوى الحماية. لذلك يعرض هذا النقص عدداً من الأخطار (أو الفرص للجاسوس) إذا كان الموظف يستخدم الحاسب المترلي لعمله.

تتضمن بعض الاهتمامات الأمنية الإضافية لحسابات النطاق العريض ما يلي:

- **عناوين IP ثابتة:** على خلاف حسابات طلب الاتصال الهاتفي، حيث يتم إسناد عنوان IP مختلف في كل مرة يتم فيها الاتصال، تزوّد حسابات النطاق العريض عادة عنوان IP ثابت للحاسب. إذا انكشف هذا العنوان سوف تحصل على هدف ثابت.
- **حالة عمل مستمرة:** بما أن حسابات النطاق العريض تكون متصلة بالإنترنت دوماً، فإن الحاسب معرّض ضمنياً للهجوم عند تشغيله.
- **وصول العائلة:** حتى لو كان المستخدم الحاسبي الأساسي يتّبع إجراءات أمنية قوية لردع المهاجمات، فقد لا يقوم باقي أفراد عائلته بإتباع الإجراءات نفسها، مما يزيد فرص الاختراق الناجح.

ومع ذلك لا داعي لتعود إلى استخدام حساب طلب الاتصال الهاتفي. يمكن تخفيف أخطار الهجوم الشبكي باستخدام بعض التقنيات التي ستمر معنا في فقرة "الإجراءات المضادة" من هذا الفصل.

أساليب: تحليل حركة المرور

يستطيع المتنصت أن يتجسس عليك، حتى لو قمت بتشفير بريدك الإلكتروني، مستخدماً تقنية تسمى تحليل حركة المرور. تتألف عملية تحليل حركة المرور من تسجيل وتحليل المعلومات، مثلاً أوقات إرسال واستقبال الرسائل، إلى من تم إرسال الرسالة، وحجم الرسائل. يمكن من خلال هذه المعلومات مقارنة بالأحداث الماضية أو الحالية أن تتوقّع بماذا يمكن أن ترتبط هذه الرسائل. عندما تصدر الحكومة تحذيراً إرهابياً مبنياً على "محادثة"، يكون هذا بسبب تحليل حركة المرور الذي كشف زيادة في تبادل الرسائل من قنوات الاتصال الإرهابية المعروفة مسبقاً (سواء البريد الإلكتروني، الراديو، الهاتف، أو غرف الدردشة). قد يعني الاتصال المتزايد عن قرب وقوع الهجوم عند استلام التعليمات النهائية (أو قد يعني أيضاً أن الإرهابيون يشنون حملة تزييف للمعلومات لأنهم يعلمون أن تحليل حركة المرور قد طُبق على شبكات الاتصالات لديهم).

مثال من العالم الواقعي لتحليل حركة المرور غير المرتبط بالحواسب، هو فهرس البيتزا الخاص بالبنتاغون.

وفقاً لمالك سلسلة مطاعم Domino's Pizza في واشنطن Frank Meeks، تزايدت توصيلات البيتزا الليلية إلى البنتاغون والبيت الأبيض أثناء المرور بفترة حرجة لأزمة عالمية. وقد صرّح Meeks "ارتفعت توصيلات البيتزا إلى الحكومة بشكل غير معقول، أثناء اجتياح كل من Panama و Grenada، بداية حرب الخليج، وحوادث عالمية كبيرة أخرى." لذلك يمكن أن تعد توصيلات البيتزا، ومع أنك قد لا تعلم التفاصيل الدقيقة لما يحدث في غرف الاجتماعات والتخطيطات، لكنك تعلم أنه شيء ضخم. وإذا كنت مطلعاً على الأحداث الجارية، يمكنك أن تخمن بعض التوقعات الدقيقة للنتائج المحتملة.

مضبوط: John Deutch ووكالة الاستخبارات المركزية CIA

ترأس John Deutch وكالة الاستخبارات المركزية CIA في الفترة الواقعة بين أيار (مايو) عام 1995 وكانون الأول (ديسمبر) عام 1996. بالتأكيد لن تصبح مدير CIA من خلال قراءتك مقالات للجواسيس في مجلة ما (انظر www.lambiek.net/prohias_antonio.htm)، لكن يجب أن تتعجب في بعض الأوقات.

بعد مرور عدة أيام من المغادرة الرسمية لمدير CIA، تم اكتشاف مواد سرية على حاسبه التابع للحكومة والموجود في مكان إقامته في Bethesda، Maryland. لقد كان من المفترض أن يكون هذا الحاسب للاستخدام غير السري، وإذا لم يكن هذا الأمر سيئاً كفاية، استخدم Deutch الحاسب للوصول إلى الإنترنت، كما كان من المعروف أن اثنان على الأقل من أفراد عائلته كانا يستخدمانه بصورة دورية. (كان Deutch مولعاً بحواسب Macintosh. تضمنت الحواسب

الخمسة الصادرة من الحكومة بطاقات للقراءة PCMCIA للمحركات الصغرية ذات الحجم 170MB والتي كان يقوم باستبدالها جيئة وذهاباً بين حواسب المكتب والمنزل).

بالرغم من أنه كان عليه أن يدرك بشكل أفضل مخاطر التجسس، فقد كشف التحقيق أن Deutch كان يعمل مع مستندات سرية على حواسب غير مؤمنة. قام "فريق الاستغلال التقني" التابع لوكالة CIA، باسترداد معلومات سرية من عدد من حواسب Deutch غير السرية ومن ضمنها أنباء سارة حول عملية سرية، اتصالات استخباراتية سرية للغاية، وميزانية برنامج الاستطلاع القومي. صرحت التحقيقات أنه من الصعب تحديد إذا تم كشف أي من هذه المعلومات السرية، لكنها أكدت من جهتها عن احتمال تعرض الحواسب لمهاجمات فيزيائية أو شبكية.

وفي عام 1999، تم تجريد Deutch من التصفية الأمنية من قبل رئيس وكالة الاستخبارات المركزية CIA الجديد George Tenet. استمر المدعون الفدراليون بمطاردة Deutch وعرضوا عليه صفقة، حيث يقوم بالاعتراف بذنبه بالاحتفاظ بالأسرار الحكومية على حواسب منزلية غير محمية، لكن لا يعاقب بالسجن. وقد وقّع Deutch، في التاسع عشر من كانون الثاني (يناير) عام 2001، اتفاقية الاعتراف بالجريمة للحصول على عقوبة مخففة، وقبل بالعقوبة ووافق على دفع غرامة بقيمة 5,000 دولار أمريكي. وفي اليوم التالي ليومه الأخير في المكتب، فاجأ الرئيس بيل كلينتون Bill Clinton وزارة العدل ووكالة الاستخبارات المركزية بمنح Deutch عفواً رئاسياً كاملاً.

John Deutch حالياً عضو كلية في قسم الكيمياء في شركة MIT.

يتوفر التقرير غير السري الكامل للتحقيق الداخلي لوكالة الاستخبارات المركزية CIA في قضية John Deutch، على الرابط www.fas.org/irp/cia/product/ig_deutch.html.

أساليب الجواسيس

والآن بعد الابتعاد عن المفاهيم الأساسية للتنصت الحاسبي، حان الوقت للدخول إلى بعض التفاصيل واستكشاف نقاط الضعف والثغرات. في هذه الفقرة سوف تتنكر بدور عميل مدرّب تقنياً (TTA) لصالح مكتب التحقيقات الفدرالي. مهمتك الحالية هي التحقيق في شخصية إرهابي أجنبي مشتبه به في مدينة أمريكية كبيرة. لقد منحتك المحكمة أمراً بالتنصت بموجب القرار FISA (ارجع إلى الفصل الثاني لمزيد من المعلومات عن هذا القرار) ولديك الموافقة الكاملة لاستخدام المراقبة السرية ضد المشتبه به. ومهمتك هي مراقبة جميع النشاطات الحاسبية الشبكية التي قد يقوم بها. من الطبيعي أن تستخدم النظام DCS-1000 (الذي كان يسمى سابقاً Carnivore)، لكن قام أحد ما بتسريب الشيفرة المصدرية على شبكة الإنترنت منذ عدة أسابيع، واكتشف مبرمج روسي خطأ فيضان التخزين المؤقت الغامض والذي تقوم بتدمير النظام. وبعد فترة قليلة

تم إصدار برامج نصية للثغرات على المنصات المتعددة ونُشرت هذه القصة على الموقع Slashdot (slashdot.org). ويبدو حالياً أن الجميع يحاولون تدمير الأنظمة DCS-1000 الحقيقية أو التخيلية والتي يشكون أنه تم تثبيتها على مزود خدمة الإنترنت لديهم. اعتقل المكتب مؤقتاً جميع الوحدات من الحقل لإعادة هندستها، لذلك يجب أن تنجز مهامك بالطريقة القديمة الطراز. (لمزيد من المعلومات عن النظام DCS-1000/Carnivore التابع لمكتب التحقيقات الفدرالي، راجع الفصل الثالث عشر، لم نتعرض لخطأ فيضان التخزين المؤقت الخيالي).

استغلال نقاط الضعف

تذكر قبل البدء بتنفيذ مهمتك الوطنية ومحاولة اقتحام حاسب الهدف عبر الإنترنت، أن التجسس الحاسي هو جمع المعلومات سرياً دون الإمساك بك. وفيما يلي بعض النصائح العاقلة التي يجب أن تتذكرها قبل أن تبدأ بإطلاق أدواتك إلى ساحة المعركة، وتحاول كشف حركة مرور الشبكة أو أن تخترق النظام:

- لا تقوم بشن مهاجماتك من حاسب يشير عنوان IP له إليك مباشرة.
- الافتراض دائماً أن رقم الهاتف الذي تتصل منه للدخول إلى الإنترنت يمكن أن يُسجل.
- الإدراك الكامل ما هي الآثار التي يمكن أن تتركها على الحاسب إذا استطعت اختراقه بنجاح.
- امتلاك الفهم الكامل لمبدأ عمل أنظمة كشف اختراق الشبكات IDS (Intrusion Detection Systems).
- الافتراض الدائم أنه بعد أن تخترق النظام، قد تتم مراقبة نشاطاتك.
- عدم قضاء وقت طويل على النظام الذي قمت باختراقه.
- إذا كنت تعمل لصالح وكالة قوى قانون وتعمل مع مزود خدمة الإنترنت لمراقبة المجرم المشتبه به، قم بحصر عدد الموظفين في مزود الخدمة الذين تتصل بهم وأكد الحاجة إلى السرية التامة أثناء إجراء التحقيقات.
- اعتماداً على الهدف، من الممكن جعل الهجوم يبدو كأنه عمل مخرّبين وليس جواسيس. فإذا تم كشفك نأمل أن يعتقد الهدف أنه عمل أطفال.

لكن بما أنك عميل ذو مستوى عالٍ من التدريب التقني، بالتالي لديك فكرة عن الأمن التنفيذي وما إلى ذلك. لذلك سوف نتقدم ونتعرف على بعض الطرق لاختراق الحواسب المتصلة بشبكة.

إجراء أبحاث عن الهدف وعمليات مسح نقاط الضعف

تماماً كأي مظهر آخر من مظاهر التجسس، تحتاج إلى إجراء بعض الأبحاث قبل البدء بتنفيذ مهمتك. في هذه الحالة، سوف تكون الأبحاث على حاسب الهدف المتصل بالشبكة (سوف نفترض أنها شبكة الإنترنت، لكنها قد تكون شبكة إنترانت Intranet مشتركة). عموماً هذه العملية تتكون من ثلاث خطوات وهي:

- **موقع الهدف**: قبل أن تتمكن من تنفيذ هجوماً حاسبياً لحاسب، عليك معرفة موقعه. ما لم تكن تعلم مسبقاً عنوان IP للهدف، يمكنك استخدام البروتوكول ping وعملية مسح المنفذ لاكتشاف الهدف المحتمل.
- **التعرّف على نظام التشغيل**: بعد أن تقوم بتحديد موقع الهدف، الخطوة التالية هي تحديد نوع نظام التشغيل والخدمات التي تعمل.
- **مسح نقاط الضعف**: بعد أن يتم تحديد موقع الهدف والتعرف عليه، الخطوة التالية هي التحقق من وجود أية نقاط ضعف يمكن استغلالها.

لنتعمق أكثر في كل خطوة من الخطوات السابقة.

موقع الهدف: كما تحتاج إلى معرفة عنوان الشارع للهدف لإنجاز مهمة الحقيبة السوداء، تحتاج أيضاً إلى معرفة عنوان IP (في هذه الحالة) للحاسب الهدف قبل أن تبدأ بالهجوم. لقد حالفك الحظ لأن الإرهابي المشتبه الذي تتعقبه يملك حساب DSL ذو عنوان IP ثابت والذي حصلت عليه مسبقاً من مزود خدمة الإنترنت المتعاون معك.

يتم اكتشاف عناوين IP غالباً باستخدام برامج مسح خدمية مؤتمتة، وخاصة الأدوات التي تقوم بعمليات المسح باستخدام بروتوكول ping ومسح المنفذ.

- **المسح باستخدام البروتوكول ping**: يتضمن هذا المسح إرسال حزم معلومات إلى عناوين IP لمعرفة إذا كان الحاسب يستجيب. يتم تطبيق هذا المسح باستخدام برنامج خدمي الذي يرسل طلب صدى إلى الهدف المحتمل من خلال بروتوكول التحكم برسائل الإنترنت ICMP (Internet Control Message Protocol). إذا تلقت الخدمة رداً فإنها تقوم بتسجيل عنوان IP. هذه الطريقة غير موثوقة تماماً لأن الحاسب الهدف قد يرفض طلب البروتوكول ping لتجنب عملية الكشف.
- **مسح المنفذ**: وهو محاولة لاكتشاف موضع الحاسب عن طريق تحديد فيما إذا كانت الخدمات تعمل على عنوان IP المطلوب. تملك خدمات مختلفة منافذ مرتبطة بها (مثلاً، يرتبط

المنفذ 80 بالبروتوكول HTTP وملقمات الويب، أما المنفذ 23 فهو مرتبط بالبروتوكول Telnet). إذا اكتشفت أداة المسح منفذاً فهي تقوم بتسجيل عنوان IP وسوف يكون لديك هدف حيوي. أدوات مسح المنفذ مفيدة جداً لأنه قد تملك الخدمة التي تم تحديدها ثغرة يمكنك استغلالها لاختراق الحاسب الهدف.

يقوم المخرّبون (crackers) بالبحث عن الأهداف عن طريق إجراء مسح لمجموعات عشوائية لعناوين IP، بحثاً عن أي أهداف محتملة. بينما الجواسيس انتقائيون أكثر بقليل، فهم يستهدفون عنوان IP وحيد تم الحصول عليه بطرق أخرى (مثل الهندسة الاجتماعية أو باستخدام تطبيق حصان طروادة) أو مجموعة معروفة من عناوين IP التابعة لمؤسسة مستهدفة.

تذكر أنه قد يحمي جدار الحماية وجود الحاسب (وخاصة إذا كان متصلاً بالإنترنت ولا يقوم بتنفيذ أية خدمات تدعم الاتصالات الخارجية)، وقد يعيد المسح القياسي عن عدم وجود حاسب ذو عنوان IP محدد، مع أنه يكون موجوداً فعلياً. إلى جانب ذلك، قد يكشف المسح عبّارة مشتركة محمية باستخدام جدار حماية ومجموعات من الاتصالات الشبكية القادمة على منافذ مختلفة. ومع ذلك، ليست تطبيقات جدار الحماية غير قابلة للاختراق ويمكن أن يتم تدميرها تحت ظروف معينة.

تذكر أنه سيتم كشف عنوان IP الخاص بك للحاسب الذي تقوم بمسحه وقد يتم تسجيله أيضاً، إلا إذا كنت تستخدم ماسحة منافذ تقوم بعمليات مسح خفية. قد لا تتم ملاحظة المسح البسيط، وذلك بسبب وجود الكثير من عمليات المسح عبر شبكة الإنترنت التي تحدث يومياً من قبل المخرّبين في جميع أنحاء العالم بحثاً عن الأنظمة المعرّضة للهجوم.



للحصول على لائحة كاملة للمنافذ الشائعة الاستخدام والخدمات المرتبطة بها، اتبع اللائحة الخاصة بسلطة تخصيص الأرقام Assigned Numbers Authority على الرابط www.iana.org/assignments/port-numbers. إذا كنت تستخدم ماسحة المنافذ، لا تحاول مسح جميع المنافذ الموجودة. حيث تتضمن معظم عمليات مسح المنفذ البحث عن مجموعة من المنافذ شائعة الاستخدام.

التعرّف على نظام التشغيل: بعد أن تقوم بتحديد عنوان IP للهدف ولائحة الخدمات المرتبطة به، الخطوة التالية هي تحديد نوع نظام التشغيل المثبت على الحاسب الهدف. وهذا أمر هام لتتمكن من معرفة نقاط الضعف المتوفرة التي يمكن استغلالها. توجد ثلاث طرق لاكتشاف نوع نظام التشغيل الذي يعمل على الحاسب البعيد:

- **المنافذ الفريدة:** يشير وجود منافذ محددة إلى نظام تشغيل معين. مثلاً، إذا وجدت المنفذ المفتوح TCP 2869، والمخصص للتوصيل والتشغيل العالمي، فمن المحتمل أن يكون نظام التشغيل المستخدم من قبل الحاسب على الطرف الآخر يستخدم نظام التشغيل Windows XP.
- **الشعارات:** تحوي الخدمات في معظم الأوقات شعار تعريف يتم عرضه عندما تتصل بالخدمة. مثلاً، إذا اكتشفت أن الحاسب يحوي المنفذ 25 (SMTP) بعد مسح المنفذ، يمكنك أن تستخدم خدمة Telnet لتتصل بالمنفذ. الاحتمالات هي عرض شعار مع اسم ملقم الويب وإصداره (لا يتم عادة عرض الشعارات من قبل العميل، أي لا يعرض عميل البريد الإلكتروني شعاراً عندما تتصل بالملقم). وهذا أمر مساعد لتحديد نوع نظام التشغيل الذي يتم استخدامه.
- **بصمات مجموعة البروتوكولات TCP/IP:** تختلف جميع أنظمة التشغيل قليلاً في تنفيذ مكدس البروتوكولات TCP/IP. من الممكن تحديد نظام التشغيل البعيد عن طريق تحليل حزم TCP الراجعة. تسهّل بعض الأدوات مثل Nmap، الذي سيتم شرحه في فقرة "أدوات التنصت ومعلومات الشبكة" من هذا الفصل، عملية بصمة نظام التشغيل عبر بروتوكولات TCP/IP.

مسح نقاط الضعف: بعد أن تقوم بتحديد المنافذ النشطة ونظام التشغيل، الخطوة التالية هي تحديد فيما إذا كان هناك أية نقاط ضعف يمكنك استغلالها للوصول إلى الحاسب. يمكنك إجراء عملية مسح نقاط الضعف يدوياً أو آلياً. مثلاً، كان التطبيق Sendmail لنظام التشغيل UNIX معروفاً بعدد من الثغرات الأمنية، فإذا اكتشفت أن النظام يقوم بتشغيل إصدار محدد من هذا التطبيق (والذي سيعرضه الشعار إذا اتصلت إلى المنفذ 25 عبر خدمة Telnet)، يمكنك بالتالي استخدام إصدار محدد للوصول إلى الجذر root.

بالتأكيد، التحقق اليدوي من نقاط الضعف عملية متعبة وطويلة. الطريقة الأفضل هي استخدام برنامج مجاني أو تجاري لمسح نقاط الضعف. ما عليك إلا تزويد الأداة بعنوان IP، وتستشير الأداة مكتبة لنقاط الضعف المعروفة ومن ثم تعيد نقاط الضعف الموجودة. ومن ثم تقوم بتحديد موقع الشيفرة المبرمجة خصيصاً لنقطة الضعف هذه (إما شيفرة ثنائية أو مصدرية) وتنفذها ضد الحاسب للهدف.



يعتبر أرشيف Neohapsis مكاناً ممتازاً لإيجاد المعلومات حول نقاط الضعف التي يمكن استغلالها، التي نُشرت في مجموعة من اللوائح الأمنية. للحصول على هذا الأرشيف اتبع الرابط http://archives.neohapsis.com.

مشاركة الملفات في نظام التشغيل Windows (Windows File Sharing)

بما أن هذا الكتاب يركز بصورة أساسية على التجسس الحاسبي لنظام التشغيل Windows، فمن الهام جداً مناقشة مشاركة الملفات لهذا النظام والتي تعتبر تقريباً من إحدى كبريات نقاط الضعف الشبكية. (قد تسمع بمراجع إلى مشاركة الملفات في النظام Windows وعائلة البروتوكولات NetBIOS، أو (Network Basic Input Output System). NetBios هي واجهة برمجة التطبيقات (API) والتي تكمّل النظام BIOS عن طريق إضافة وظائف خاصة للشبكات المحلية LAN. غالباً يُستخدم المصطلحان مشاركة الملفات للنظام Windows وعائلة بروتوكولات NetBIOS بشكل متبادل).

زودت شركة Microsoft، بدءاً من نظام التشغيل Windows 3.11، جميع إصدارات أنظمة Windows بإمكانية مشاركة الملفات أو المجلدات عبر الشبكة مع الحواسب الأخرى التي تستخدم النظام Windows. الآلية التحتية لمشاركة الملفات في النظام Windows هو بروتوكول نظام ملفات الإنترنت المشترك CIFS (Common Internet File System)، المعروف مسبقاً باسم بروتوكول كتل رسائل الملقم SMB (Server Message Block). يسمح البروتوكول CIFS للحاسب أن يتعامل مع الملفات على الجهاز الشبكي البعيد ذو نظام التشغيل Windows كأنها ملفات محلية (كما يدعم هذا البروتوكول أيضاً قابلية الوصل بين نظامي التشغيل Windows وUnix).

وصول الملفات الواضح هو ميزة قيمة جداً، لكن قد تعرّض المشاركات الشبكية التي تم تكوينها بشكل خاطئ ملفات النظام الحساسة للهجوم. إحدى الطرق التي انتشر من خلالها فيروس Sircam ودودة Nimda خلال صيف 2001، عن طريق اكتشافُ المشاركات الشبكية غير المحمية للنظام Windows ونسخ أنفسهم إلى هذه المشاركات. يفتح الكثير من المستخدمين دون قصد ملفاتهم إلى المتنصتين عندما يجعلون أقراصهم قابلة للقراءة والكتابة، وبالتالي يستطيع زملاء العمل وأفراد العائلة الوصول إلى هذه الملفات بسهولة. حتى لو كان النظام مكوّناً بشكل آمن، هناك عدد من الأدوات والتقنيات لاختراق المشاركات المحمية.

نتيجة لنقاط الضعف الموجودة في مشاركات الملفات للنظام Windows، فقد كان لوقت طويل هدفاً للمخرّبين، كما يستفيد الجواسيس منها لأهدافهم الخاصة. إذا تم اكتشاف منافذ نشطة لعائلة بروتوكولات NetBIOS خلال مسح المنافذ، سوف تعلم بوجود النظام Windows والذي قد يشاركُ الملفات. ومن ثم تستطيع استهدافه باستخدام أدوات شبكية للحصول على المعلومات حول هذه المشاركات، الاتصال بها بشكل مباشر، أو شن هجوم القوة العمياء لاختراق المشاركات المحمية بكلمة مرور. وإذا لم يتم تثبيت النظام فقد يحالفك الحظ في كشف الملفات الحساسة.

لكن في حالتنا هذه، تخبر رئيسك أنه لا يوجد داعٍ لشن هجوم باستخدام عائلة بروتوكولات NetBIOS للوصول إلى الملفات عن بعد. حيث أنجز الفريق عمل الحقيبة السوداء على شقة المشتبه به وقاموا بمضاعفة قرصه الصلب. كما أن نقاط الضعف لعائلة بروتوكولات NetBIOS معروفة بصورة واسعة للمخرّبين ومبرمجي الفيروسات، يقوم الكثير من مزودي خدمة الإنترنت وخاصة الخدمة ذات النطاق العريض، بحجز محاولات مسح المنافذ 137، 138، و 139 من الإنترنت. توجد تقنيات أخرى للتحقيقات يمكنك استخدامها في هذه الحالة والتي يمكن أن تكون فعالة أكثر.



لتتعلم أكثر حول مهاجمات عائلة بروتوكولات NetBIOS، تحقق من الجولة التعليمية للمخرّب والتي جمعها "القرصان الأخلاقي" Gaurav Kumar، على الرابط www.mycgiserver.com/~ethicalhackers/netbios.html.

مراقبة الشبكة

تقدم عملية التنصت على البيانات خلال مرورها عبر الشبكة جميع أنواع المعلومات المثيرة للجاسوس. البيانات غير المشفرة يمكن عرضها بسهولة، سلبياً تماماً، ودون أن يعلم الهدف أن بياناته مكشوفة.

خلال تحقيقاتك مع الإرهابي، يوجد لديك هدفان: جمع الأدلة المحتملة عن الأعمال الإجرامية وجمع الاستخبارات التي تستطيع أن تمنع حادثاً إرهابياً متوقعاً. مراقبة الشبكة هو المكان حيث يجب أن تركّز وقتك ومواردك.

برامج sniffer: وهي أداة تتنصت على حركة المرور ضمن شبكة حاسبية (يسمى أيضاً، packet sniffer، محلّل البروتوكولات protocol analyzer، أو مراقب الشبكة network monitor). إذا قمت بمراقبة حركة مرور الحزم الخام، كل ما سوف تراه هو سلسلة من البايتات المارة عبر الشبكة. هذا ليس أمراً مفيداً جداً، لذلك عليك الاستفادة من البيانات الخام إضافة إلى التقاط حركة مرور الشبكة، تقوم برامج sniffer بفك تشفير البيانات الثنائية وتحولها إلى بيانات مقروءة مبنية على البروتوكولات المرتبطة بالاتصال. مثلاً، يمكن فك تشفير طلب المستعرض إلى ملقم ويب بصورة صحيحة بحيث يمكنك قراءة المحادثة من خلال بروتوكول HTTP بين الحاسبين.

تمر حركة المرور، في شبكة Ethernet، عبر كل بطاقة شبكة مع تجاهل البطاقة المعلومات غير الموجهة إليها. (إذا كان إطار الحزمة يملك عنوان MAC مختلف عن عنوان بطاقة الشبكة، فلن تقبل البطاقة هذه الحزمة). على أية حال، يمكن إخضاع بطاقات الشبكة إلى نمط مشوش، مما

يجعل البطاقة تقرأ حركة المرور المارة عبر الشبكة. حيث يُخضع برنامج sniffer بطاقة الشبكة إلى وضع مشوش ومن ثم يلتقط البيانات المارة عبر الشبكة.

تعمل برامج sniffer بصورة ممتازة على شبكة Ethernet تقليدية والتي تتضمن موجّهات Routers ومجمّعات Hubs. لكن عندما تبدأ بتقديم المبدّلات Switches إلى تكوين الشبكة، يستقبل برنامج sniffer البيانات من الحاسب الذي تم تثبيته عليه فقط. والمبدّلات مصممة لإرسال حركة المرور الشبكية من منفذ فيزيائي إلى آخر. فهي عملياً لا ترسل حركة المرور إلى جميع الحواسب في الشبكة. لتستطيع مراقبة شبكة متبدلة، تحتاج إلى تثبيت جهاز للتنصت على الشبكة بين الحاسب ومنفذه المتبدل. يقوم جهاز التنصت بتكرار دفق البيانات بين الحاسب وبقية الشبكة. يمكن أن يوصل جهاز sniffer إلى جهاز التنصت لجمع البيانات. كما يمكنك أيضاً استخدام تقنية تسمى انتحال بروتوكول ترجمة العنوان ARP ‏(Address Resolution Protocol). كتب Tom King مقالة ممتازة حول هذه الطريقة، وتتوفر على الرابط www.sans.org/rr/netdevices/packet.php.

تستعرض معظم برامج sniffer البيانات في الزمن الحقيقي عندما يتم جمعها، أو حفظها ليتم استعراضها لاحقاً. إلى جانب ذلك، يمكن استخدام المرشحات لالتقاط أنواع محددة من حركة المرور (مثلاً، من عنوان IP محدد). في مثالنا، تستطيع تثبيت برنامج sniffer إلى مزود خدمة الإنترنت ومراقبة حركة المرور الشبكية الداخلة والخارجة المرتبطة بالمشتبه، ودون انتهاك حقوق الخصوصية لباقي الزبائن. تولّد الشبكات كمية ضخمة جداً من الضجيج مع حزم التحكم، طلبات ملقم اسم المجال DNS، والمعلومات الأخرى والتي على الأغلب غير مرتبطة بنشاطاتك التجسسية. يمكنك أيضاً استخدام المرشحات لعرض أو تخزين البيانات المرتبطة ببروتوكولات محددة مثل SMTP وPOP للبريد الإلكتروني أو HTTP لاستعراض الويب.

وسائل التجارة: برامج Carnivore التجارية

تتم مناقشة برنامج DCS-1000/Carnivore التابع لمكتب التحقيقات الفدرالي في الفصل الثالث عشر، لكن بما أننا نقوم بالتحدث عن برامج sniffer، فمن الجدير بالذكر عدة منتجات تجارية التي تقوم بإنجاز نفس نوع مراقبة الشبكة مثلما يفعل البرنامج DCS-1000. لا تحتاج إلى ميزانية ضخمة لشرائها، لكن احترس على محفظة نقودك. ومن بعض المنتجات الجديدة بالملاحظة نذكر ما يلي:

- **SilentRunner: أداة تحليل وتشبيك حديثة ومتطورة تم إنتاجها من قبل Raytheon (مقاول حكومي كبير لفترة طويلة من الزمن). لمزيد من المعلومات اتبع الرابط www.silentrunner.com.**

- **NetIntercept:** أداة تحليل وجمع بيانات أخرى مطورة من قبل شركة Sandstorm. لمزيد من المعلومات اتبع الرابط /www.sandstorm.net/products/netintercept.

- **DragNet:** تم تطويرها بالأصل من قبل شركة Traxess (والتي ملكتها فيما بعد شركة Network Associates في شهر آب عام 2002)، وتجمع بين ميزات المراقبة وتسجيل المفاتيح. كان من المفترض أن يتم إصدار المنتج عام 2003، وسوف تتوفر المعلومات عند الإصدار على الرابط www.nai.com.

- **RetrievalWare:** تجمع كميات ضخمة من البيانات مقدرة بالجيغا بايت، ومن ثم تحلل هذه البيانات وتستخلص كل ما هو مفيد. مع أنه لم يتم تصميمها خصيصاً لأغراض المراقبة، لتطبيقات التنقيب عن البيانات، مثل برنامج Convera's RetrievalWare، ويتم استخدامها من قبل مكتب التحقيقات الفدرالي ووكالات استخباراتية حكومية متنوعة. لمزيد من المعلومات اتبع الرابط www.convera.com.

إذا كنت تملك ميزانية ولديك بعض الخبرة في الشبكات ولغة البرمجة C، يمكنك في أي وقت الحصول على نسخة من برنامج Altivore، والذي كان من المفترض أن يكون إصداراً مفتوح المصدر لبرنامج Carnivore، لكنه بالكاد خرج من تصميمه الأولي. تتوفر المعلومات والشيفرة المصدرية على الرابط /www.robertgraham.com/altivore.



أعدّ Robert Graham، وهو مبرمج قديم العهد وله خبرة واسعة في الصناعة الحاسبية ومطور جدار الحماية BlackICE، لائحة شاملة بالأسئلة التي تتكرر باستمرار حول برامج sniffer على الرابط:

www.robertgraham.com/pubs/sniffing-faq.html.

تسجيلات الملقم: بالإضافة إلى الحصول على المعلومات من السلك، يمكنك أيضاً تجميع المعلومات حول حركة المرور الشبكية التي يسجلها الملقم. تزوّدك تسجيلات الملقم نموذجياً بيانات المناقلات، مثلاً عناوين IP للمصدر والوجهة، الوقت التي حدثت فيه المناقلة، والمعلومات المحددة لنوع معين من الملقمات (مثلاً، سوف يبلغ ملقم البريد عنوان البريد الإلكتروني للمرسل والمستقبل، زمن إرسال أو استقبال الرسالة، حجم الرسالة، ومعلومات أخرى). يستطيع أي شخص يتمتع بالوصول الفيزيائي أو البعيد إلى الملقم مثل مدراء النظام الشرعيين، ضباط قوى القانون الحاملين لأمر من المحكمة، أو الجواسيس الذين قاموا باختراق الأمن، الحصول على هذه البيانات. (بالإضافة إلى التسجيلات التي تولدها برامج جدار الحماية على الحواسب المنزلية أو حواسب الأعمال الصغيرة).

في حالة التحقيق في قضية الإرهابي الافتراضي، فإن مزود خدمة الإنترنت متعاون جداً وذلك بسماحه لك باستعراض مداخل تسجيلات الملقم المرتبطة بالمشتبه. من أجل حماية الحقوق الشخصية لبقية المشتركين، فإنك تقوم بالإطلاع على عنوان IP الخاص بالمشتبه فقط. كما يقوم مدير نظام نافع بكتابة برنامج نصي باستخدام لغة البرمجة Perl والذي يمرر تسجيلات متنوعة ويستخلص مداخل مرتبطة بالمشتبه به. تقوم بدورك بمراجعة سريعة للبرنامج النصي وتقترح أن يقوم مدير النظام بإضافة تابع تجزئة MD5 للبيانات التي تم استخلاصها فقط من أجل التحقق. يقوم مدير النظام بتنصيب وظيفة زمنية (الأوامر أو الأوامر النصية التي تنفذ تلقائياً في زمن أو تاريخ محدد)، ويقوم البرنامج النصي بالتنفيذ يومياً في السابعة والنصف صباحاً. ومن ثم يتم تشفير الخرج وإرساله إلى حساب بريد إلكتروني مزيف على موقع Hotmail. (قد لا يكون إرسال الرسالة إلى عنوان fbi.gov فكرة صائبة).

بما أن تطبيقات الملقمات تولد كمية ضخمة من البيانات، لذلك تُحذف ملفات السجلات بشكل دوري لتوفير المساحة على القرص. لقد منعت السجلات المحذوفة على خدمة البريد الإلكتروني لمواقع Hotmail وKinko من إجراء التحقيقات في قضية Zacarias Moussaoui، الاسم الذي أُطلق على مختطف الطائرة العشرين من هجمات 9/11 أيلول، من جمع الأدلة المحتملة لهذه القضية. لذلك تطلب أن تتم أرشفة جميع السجلات أثناء التحقيقات، لأنه في حالة تمت مقاضاة المشتبه به، سوف تلعب هذه السجلات دوراً هاماً باعتبارها جزءاً من الدليل، وبشكل أساسي لتأييد مداخل التسجيلات المجزئة التي كنت تحصل عليها يومياً.

أخيراً تشكر جميع من ساعدك أثناء التحقيق لتعاونهم، مؤكداً على أن هذه قضية أمن قومي وعلى أهمية الحفاظ على سرية التحقيق.

تفحص تجهيزات الشبكة

يمكن أن تزوّد الأجهزة الشبكية مثل الموجّهات، المبدّلات، وبرامج جدار الحماية (سواء برمجيات أو تجهيزات) معلومات حول نشاطات الهدف. وهذا الأمر صحيح بصورة خاصة في الشبكات المترلية والشبكات المكتبية الصغيرة، حيث لا يمتلك المستخدمون خلفية تقنية كافية لفهم المخاطر التي قد يتعرضون لها.

تفحص ملفات التسجيل: تحتفظ هذه التطبيقات والأجهزة الشبكية بسجلات عن الاتصالات الشبكية الداخلة والخارجة. وقد تشكّل السجلات مصادر معلومات قيّمة لمعرفة ما هو نوع النشاط الشبكي الذي يقوم به أحد المستخدمين. تتضمن ملفات التسجيل نموذجياً التاريخ والوقت، عناوين IP للمصدر والوجهة، وأرقام المنافذ (والتي سوف تمنحك فكرة عامة عما يفعله الشخص المستهدف، مثال، يعني النشاط على المنفذ 23 اتصال SSH مشفّر).

تخزن بيانات التسجيل على ذاكرة الجهاز ويتم الوصول إليها فيما بعد باستخدام تطبيق برمجي يرتبط مع الجهاز الصلب. ثم تُنقل البيانات في الذاكرة إلى ملف تسجيل مخزن على القرص الصلب على حاسب المستخدم. تحتفظ منتجات جدار الحماية البرمجية افتراضياً بملف سجل نصي أو ملفات سجل للاتصالات الشبكية. كثير من المستخدمين لا يدركون هذا الأمر، لذلك يتجاهلون التعامل مع سجلات المبدّل أو جدار الحماية والذي يعرض المواقع التي كانوا يقومون بزيارتها، ومتى كانوا يتصفحونها، عندما يزيلون آثار استعراض مواقع الإنترنت على مستوى المستعرض.

مضبوط: الحيل السياسية الدنيئة

خلال حملة انتخاب مجلس الشيوخ في مقاطعة Minnesota عام 2000، تم إرسال سلسلة من الرسائل الإلكترونية إلى المنتخبين الديمقراطيين تحثهم على عدم دعم المرشح Mike Ciresi في حفلة اجتماع ترشيح الولاية. حيث هاجمت الرسائل الإلكترونية Ciresi ووصفته بأنه ضد الاتحاد وضد البيئة. أرسلت الرسالة من حساب Hotmail (kylomb@hotmail.com) وكانت من عضو حزب "committed progressive" واسمها Katie Stevens.

لكن عندما بدأ موظفو Ciresi بالتحقيق، لم يتمكنوا من إيجاد Katie Stevens.

بدأت الأدلة تشير إلى السيناتور الجمهوري المنافس للمرشح Mike Ciresi، وهو Rob Grams. لقد كانت حملة Grams مدارةً من قبل Christine Gunhus، والتي كانت خطيبته. عندما تم فحص الرسائل الإلكترونية الثلاثة، أشارت سلسلة من العلامات إلى تورط Gunhus بحملة مليئة بالحيل القذرة.

تضمنت بعض الرسائل الإلكترونية ملفات Microsoft Word مرفقة، وكان اسم المؤلف في خصائص المستند هو Christine Gunhus. (يدخل برنامج Word آلياً هذه المعلومات، بناء على هوية المالك المسجل للبرنامج). الضربة الأولى

تملك رسائل Hotmail ترويسة لتوليد عنوان IP والتي تعرض عنوان IP المتولد عن الرسالة. أظهرت الرسائل الأولى أنه تم إرسالها من محطة العمل pay-by-the-minute من مركز النسخ Kinko. أرسلت الرسائل التالية من حساب WorldNet باسم AT&T، لكن احتفظ هذا الحساب بسجلات بيانات المتصل لجميع الاتصالات القادمة إلى أجهزة المودم. عندما طالبت السلطات السجلات المرتبطة بعنوان IP المتولد في الإطار الزمني الذي أرسلت فيه الرسالة، وجدوا أحد الأرقام الهاتفية المستخدمة للوصول إلى خدمة طلب الاتصال الهاتفي تخص Christine Gunhus. الضربة الثانية.

استخدمت Gunhus إصداراً قديماً من برنامج Word والذي كان يحشر ما يسمى بالمعرف الوحيد العمومي GUID (Global Unique Identifier). تضمن هذا المعرف GUID رقم MAC لبطاقة الشبكة إذا كانت مثبتة. وبما أن أرقام MAC وحيدة لذلك فقد يرشد المعرف GUID أحداً ما إلى الحاسب الذي أنشأ المستند (أو على الأقل بطاقته الشبكية). عندما أصدرت الشرطة مذكرة تفتيش لشقة Gunhus، وجدوا أن رقم MAC لبطاقتها الشبكية يطابق رقم MAC الذي سجله المعرف GUID على المستندات المرسلة باستخدام البريد الإلكتروني. الضربة الثالثة، قضي عليك.

تعتبر هذه الحيل الدنيئة التي قامت بها Christine Gunhus جريمة بموجب قرار الممارسات العادلة للحملات في ولاية Minnesota، والتي تمنع الحملات من نشر معلومات مجهولة. وفي شهر حزيران (يونيو) عام 2001، لم تحتج Christine Gunhus على الإهانة وتمت تصفيتها، قرر المدعون ألا يضغطوا على عقوبة السجن. خسر Ciresi المنصب الأول في حزبه (ليس بسبب رسائل Gunhus، بل نتيجة الحملة القوية من قبل منافسه Mike Dayton)، وخسر Grams في النهاية الانتخابات العامة وفشل في استرداد مقعده في مجلس الشيوخ.

استغلال كلمات المرور الافتراضية

تملك معظم الأجهزة الشبكية كلمة مرور للحد من الوصول إلى الميزات الإدارية للجهاز، وفي كثير من الحالات، لا يغير المستخدم أو مدير النظام كلمة المرور الافتراضية بتاتاً. وهذه مجازفة بحد ذاتها بسبب توفر لوائح بكلمات المرور الافتراضية بصورة واسعة على شبكة الإنترنت. إذا استطعت أن تحدد ما هو نوع الجهاز الشبكي المستخدم ومن ثم تمكنت من الوصول إليه محلياً أو عن بعد باستخدام كلمة المرور الافتراضية، يمكنك تغيير الإعدادات الأمنية أو الوصول إلى المعلومات المخزنة على القرص الصلب.



للحصول على لائحة شاملة ومحدثة لكلمات المرور الافتراضية لعدد من التجهيزات المختلفة، اتبع الرابط www.phenoelit.de/dpl/index.html.

مهاجمات شبكية أخرى

بالإضافة إلى اقتحام الحاسب من خلال الشبكة، استخدام برامج sniffer، أو تفحص سجلات الملقم، توجد مهاجمات شبكية أخرى يمكنك تنفيذها من أجل الحصول على البيانات المطلوبة، ومن ضمنها ما يلي:

التطبيقات الخبيثة: طريقة أخرى لمراقبة الشبكة هي تنصيب أحد أنواع التطبيقات الخبيثة على الحاسب الهدف والتي تجمع المعلومات (سواء كانت من حركة مرور الشبكة أم لا)، ومن ثم يرسل التطبيق هذه المعلومات إليك. هناك مسجلات مفاتيح تجارية، مرت معنا في الفصل الثامن، تستطيع تنفيذ هذه المهمة، بالإضافة إلى تطبيقات حصان طروادة، التي ناقشناها في الفصل التاسع.

يمكن تثبيت التطبيقات الخبيثة إما من خلال عمل الحقيبة السوداء أو عن بعد بنفس الطريقة التي تنتشر فيها الدودة أو الفيروس، مثلاً من خلال ملف مرفق برسالة إلكترونية. في حالة الإرهابي المشتبه به، يكون عمل الحقيبة السوداء ملائماً، مثل العمل الذي أنجزه مكتب التحقيقات الفدرالي في حالة المجرم Nicodermo Scarfo. (لا توجد معلومات فيما إذا كان مسجل المفاتيح الذي تم استخدامه يتمتع بإمكانية إرسال البيانات عن بعد، و لم يتم كشف أي معلومات عن مسجل المفاتيح، ما لم يحصل تسرب للمعلومات أو طلب من قبل قرار حرية المعلومات بتزويد بعض الإشارات في المستقبل).

هذا النوع من التطبيقات الخبيثة مفيد بشكل خاص في الحواسب ذات الاتصال ذو النطاق العريض، لأنها تظل متصلة بالإنترنت وتستطيع إرسال البيانات بسهولة في أي وقت، مثلاً عندما يكون الهدف نائماً ولا يلاحظ وقوع هذه النشاطات الشبكية. السيئة الأساسية لهذا النوع من الهجوم هو أن الهدف الذكي سوف يستخدم تطبيقات جدار الحماية وإجراءات مضادة أخرى والتي سوف تكشف وتدمر التطبيق الخبيث بسهولة بعد تثبيته.



أحد الأمثلة التقليدية للتطبيق الخبيث هي أداة اتصال شبكي تسمى Stealth Email Redirector (SER). بعد تثبيت الأداة، ترسل آلياً نسخة من البريد الصادر المار عبر المنفذ 25 (SMTP) إلى عنوان بريد إلكتروني محدد (تأكد من استخدامك حساباً مزيفاً صعب التعقب). تتوفر معلومات حول هذا المنتج على الرابط /www.softsecurity.com/products/ser.

مواقع ويب خبيثة: إلى جانب وجود شيفرة خبيثة مثبتة مباشرة على الحاسب، توجد شيفرة خبيثة يتم تنفيذها عند زيارة موقع ويب. يشكل برنامج مستعرض الإنترنت Internet Explorer حالياً المستعرض الأكثر استخداماً، ولسوء الحظ فهو يتمتع بسمعة متبدلة كثيراً لامتلاكه عدداً من الثغرات الأمنية. حيث تشكّل عناصر تحكم ActiveX الخبيثة نقاط ضعف للبرامج النصية النشطة، ثغرات في آلة جافا الافتراضية Java Virtual Machine، وأخطاء فيضان التخزين للمكدس، بعض التقنيات التي يستطيع الجاسوس استغلالها في صفحة ويب مصممة خصيصاً

لسرقة المعلومات المخزنة على القرص الصلب بعد فتح الصفحة. قد تكون شيفرة موقع الويب انتقائية جداً وتُنفذ ضد عنوان IP معروف أو أجزاء أخرى من معلومات المستخدم التي يتم استخلاصها من المستعرض. إن جعل الهدف يقوم بزيارة صفحة الويب يعتمد على الهندسة الاجتماعية ، إما عن طريق البريد الإلكتروني أو الهاتف.

يمكن أن تكون هذه المهاجمات فعالة جداً لعد أسباب:

- لا يدرك معظم المستخدمين خطر هذا النوع من صفحات الويب، على خلاف الفيروسات.
- من الصعب جداً كشف هذا النوع من الهجوم، إذا تم تنفيذه بصورة صحيحة.
- لا يستخدم معظم الناس الترميمات الأمنية لمواجهة نقاط الضعف.



للحصول على قائمة شاملة للثغرات الأمنية الحديثة التي تم ترميمها والتي لم ترمم بعد لمستعرض الإنترنت Internet Explorer والتي يمكن أن يستخدمها الجاسوس، اتبع الرابط /pivx.com/larholm/unpatched.

طرفيات الإنترنت ذات الوصول العام والشبكات: أحد الأمور التي يمكنك استغلالها لأغراض التجسس تدور حول الشعبية المتزايدة لمقاهي الإنترنت، المكتبات، الفنادق، وأكشاك الإنترنت والتي توفر طريقة رخيصة وسهلة للاتصال بالإنترنت. تسمح هذه المصادر العمومية المناسبة للأشخاص المشغولين بتفقد بريدهم الإلكتروني وبتصفح شبكة الإنترنت وهم خارج المترل. بعض التقنيات التي يمكن أن تستخدمها لكشف المعلومات الحساسة:

- **استراق النظر:** أي مراقبة أحد ما عندما يقوم بإدخال اسم حسابه وكلمة المرور على لوحة المفاتيح. وتتوفر هذه الفرصة في أي مقهى إنترنت (يجب ألا تفضح نفسك أثناء قيامك بهذا). حتى لو لم تستطع رؤية المفاتيح كاملة، يمكنك مع ذلك تضييق الاحتمالات بمراقبة موقع الأصابع عندما يتم إدخال المفاتيح وبإحصاء عدد ضربات المفاتيح. يمكن تطبيق هذه المهارة عندما يقوم أحدهم بتسجيل الدخول.
- **مسجلات المفاتيح:** يمكن تنصيب مسجلات مفاتيح برمجية أو صلبة بسهولة على الحواسب العمومية لتسجيل البيانات التي يدخلها المستخدم. ارجع إلى الفصل الثامن لمزيد من المعلومات حول مسجلات المفاتيح.
- **الوصول إلى الشبكة والملقم:** قد تمنح أوامر المحكمة، الرشوة، الهندسة الاجتماعية، التخريب، أو مجرد الفضول، أحداً ما الوصول إلى الشبكة. وقد وردت تقارير من بعض الفنادق الأوروبية عن قيامها بمراقبة حركة الإنترنت للمسافرين من أجل الأعمال على

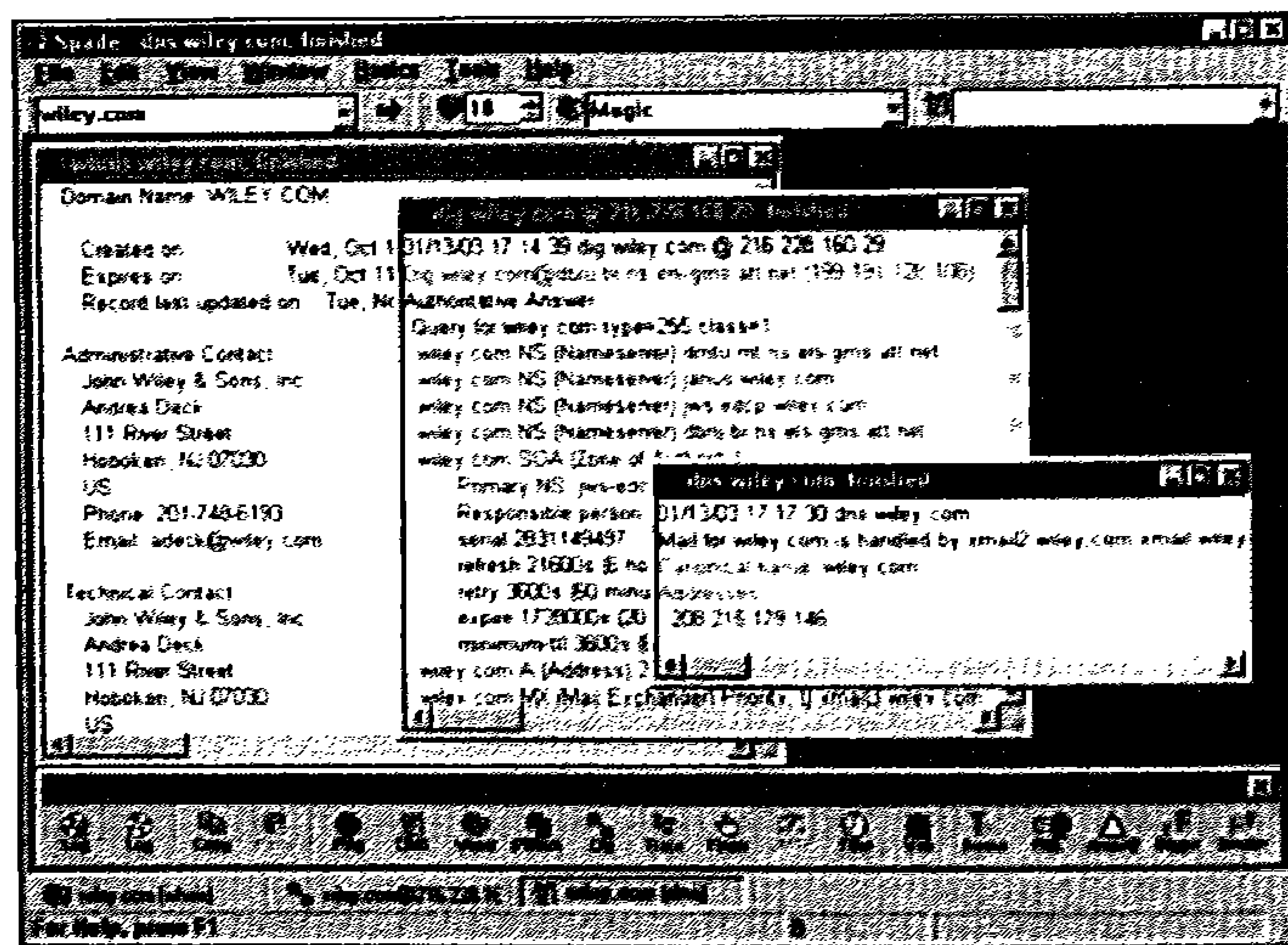
حواسب الفنادق أو الاتصالات الشبكية بهدف التجسس الاقتصادي بأمر من حكوماتها. بحث مكتب التحقيقات الفدرالي في الولايات المتحدة عن المعلومات من مزودات خدمة الإنترنت لإجراء التحقيقات.

أدوات التنصت والمعلومات الشبكية

والآن بعد أن حصلت على بعض المعرفة الأساسية لبعض نقاط الضعف والمهاجمات التي يمكنك شنها على الحواسب الشبكية، حان الوقت لتتعرف على بعض الأدوات المعينة التي يمكنك استخدامها لتسهيل مهمة المراقبة عليك. معظم هذه الأدوات مجانية ومتوفرة للعامة ولا تحتاج إلى مصاريف كبيرة لتحميلها من الإنترنت.

SAMSPADE

SamSpade وهي أداة مجانية للاكتشاف والحصول على معلومات الشبكة (انظر الشكل 10-1)، كما تتضمن عدداً من الأدوات الشبكية مثل whois، tracert، ping، و dig والتي يمكن أن تستفيد منها لاكتشاف المعلومات حول الحواسب الشبكية. وهي أداة قيّمة جداً لإجراء البحث عن أهداف محددة. يمكنك تحميل هذه الأداة من الرابط www.samspade.org. كما يوفر الموقع نفسه إصدارات متصلة لأدوات برمجية، وهذا في حالة كونك في مكان ما متصلاً بالشبكة ولا تملك معك أدوات موثوقة.



الشكل (10-1) برنامج SamSpade، يظهر بيانات متنوعة مرتبطة بشبكة شركة مستهدفة. يفيد هذا النوع من المعلومات في تخطيط هجوم شبكي.

NMAP

تشكّل الأداة Nmap الخيار الأفضل لخبراء الأمن وللجواسيس لمسح المنافذ. وهي اختصار للعبارة Network Mapper، وهي أداة مجانية مفتوحة المصدر مبرمجة من قبل Fyodor، وتستطيع تحديد موقع الحواسب المستهدفة، الاستعلام عن الخدمات التي يتم تنفيذها عليها، والتعرّف على أنظمة التشغيل التي تعمل على هذه الحواسب.

ما يميز الأداة Nmap عن بقية منتجات مسح المنافذ قدرتها على استخدام عدد من الطرق المختلفة لاكتشاف المعلومات حول الحاسب الهدف. وتتمتع الأداة ببعض تقنيات المسح مثل صعوبة كشفها حتى عندما تتضمن الحواسب الهدف أنظمة كشف اختراق الشبكات IDS (Intrusion Detection Systems). إحدى هذه التقنيات تسمى Idlescan تسمح للمهاجم أن يستكشف الحاسب الهدف من دون أن يتم كشف عنوان IP عن طريق حشر حزم من مضيف غير متعمد.

هذه الأداة كانت بالأصل على شكل سطر للأوامر والتي كانت تنفذ على أنظمة Unix فقط، لكن تم مؤخراً تطوير إصدار للنظام Windows. يمكنك تحميل النسخة الأصلية للأداة لنظام Unix من الموقع /www.insecure.org/nmap، وكذلك النسخة الخاصة للنظام Windows من الموقع www.nmapwin.org.

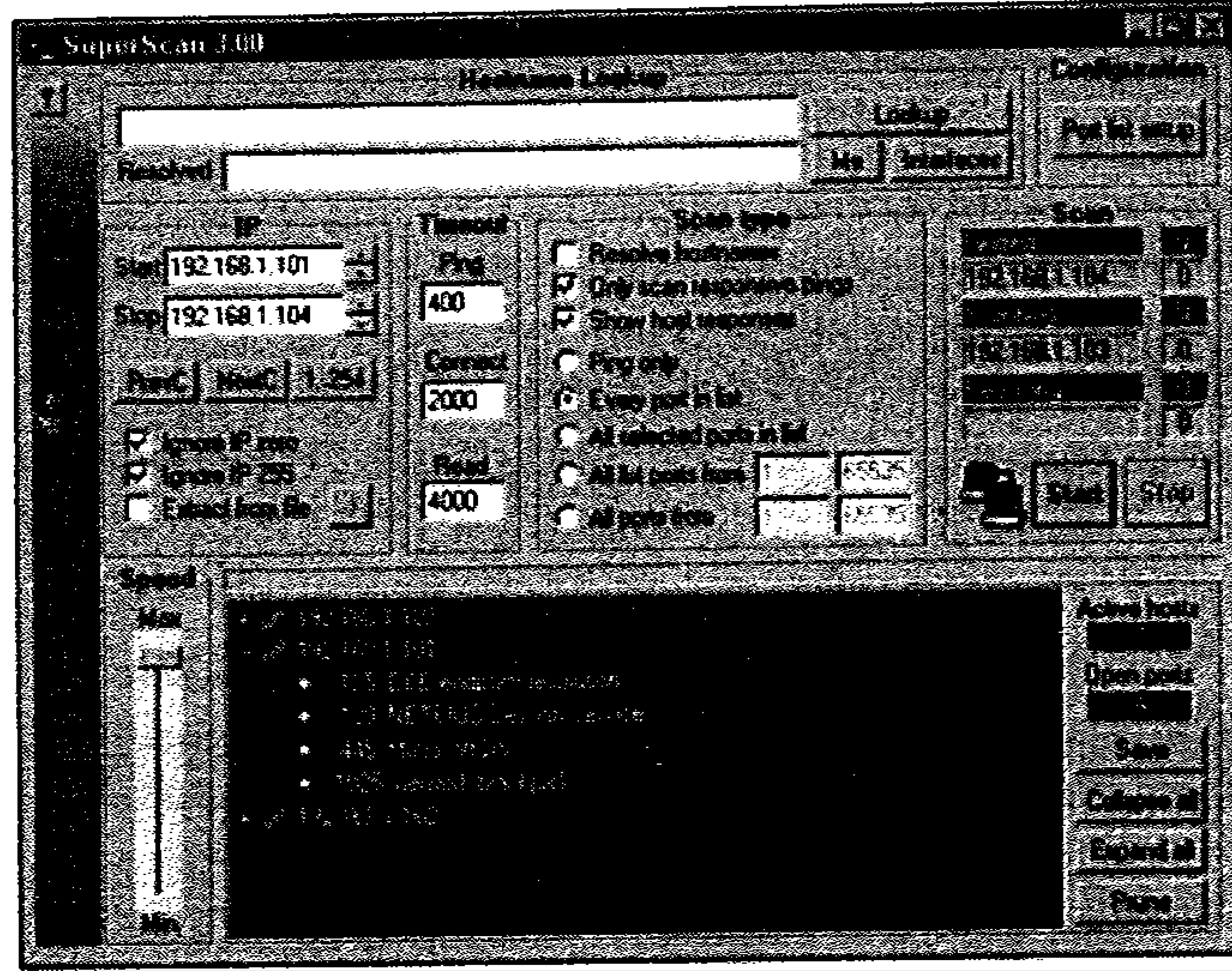
SUPERSCAN

إذا لم تكن مهتماً ببقائك مخفياً (مع أنه يجب أن تكون كذلك)، لكنك تبحث عن ماسح منافذ TCP سريع وسهل الاستخدام، تحقق من الأداة SuperScan لشركة Foundstone (انظر الشكل 10-2). الأداة مجانية ويمكن تحميلها من الرابط:

www.foundstone.com/knowledge/proddesc/superscan.html.

NESSUS

وهي أداة أمنية لمسح المنافذ مفتوحة المصدر، مبرمجة من قبل Renaud Deraison وهي موجودة منذ عام 1998. تتضمن الأداة Nessus مكوّن وهو الملقم والذي ينفّذ التدقيقات الأمنية ومكوّن آخر هو العميل والذي يمثّل واجهة المستخدم. كما تتميز هذه الأداة بوجود مكتبة شاملة لنقاط الضعف التي يمكن الاستفادة منها. كما وُجدت أكثر من 1,100 وظيفة إضافية متوفرة يمكن تحميلها، في شهر كانون الثاني (يناير) عام 2003، لمعرفة وجود عدد من المساوئ الأمنية في عدد من الأجهزة وأنظمة التشغيل. كما تتم إضافة برامج نصية إضافية بشكل مستمر عند اكتشاف ثغرات جديدة.



الشكل (10-2) ماسحة المنافذ SuperScan، وهي تظهر الحواسب والمفتوحة على شبكة محلية متصلة بموجّه.

بعد أن تقوم بتكوين المكونين الملقم والعميل، ما عليك سوى إدخال عنوان IP للحاسب الهدف (تستطيع الأداة Nessus العمل مع الأداة Nmap لإنجاز مسح للمنافذ بشكل خفي)، اختيار نوع الاختبارات الأمنية التي تريد تنفيذها، وسيفحص البرنامج Nessus الهدف بحثاً عن الثغرات. عند الانتهاء من المسح، تولد الأداة تقريراً كاملاً يعرض الثغرات التي تم اكتشافها، المراجع الخارجية، وحلول لإصلاح المشكلة.

السيئة الأساسية لمستخدمي نظام التشغيل Windows هي أن مكوّن الملقم متوفر فقط للأنظمة المتوافقة مع Unix. ومع ذلك فهي أداة قيّمة كفاية لتقتنع بتثبيت نظام التشغيل Linux فقط لكي تستخدمها. للحصول على مزيد من المعلومات وتحميل الأداة المجانية، اتبع الرابط www.nessus.org. (إذا كنت تحتاج بدون شك لأداة مسح للنظام Windows، يجب أن تستخدم المنتجات التجارية المكلفة مثل أداة المسح Internet Security Systems' Internet Scanner، لمزيد من المعلومات عنها اتبع الرابط www.iss.net).

أدوات عائلة بروتوكولات NETBIOS

يوجد عدد من الأدوات لكشف الحواسب باستخدام مشاركة الملفات في النظام Windows. من أشهر أدوات الهجوم باستخدام عائلة بروتوكولات NetBIOS:

- NAT (NetBIOS Auditing Tool): وهي أداة سطر الأوامر تحدد مشاركات عائلة بروتوكولات NetBIOS وتنفذ هجوم القوة العمياء لكلمات المرور. هذه الأداة مجانية ويمكنك تحميلها من الرابط http://online.securityfocus.com/tools/543.
- LEGION: يشبه في وظيفته الأداة NAT، لكن تمت برمجته بلغة Visual Basic وله واجهة استخدام للنظام Windows. طُورت هذه الأداة من قبل المجموعة الأمنية Rhino9 غير الموجودة حالياً، وكانت نصف مجانية في وقت إصدارها عام 1997. بالرغم من قدم هذه الأداة إلا أنها لا تزال فعالة مع الإصدارات الحالية للنظام Windows، ويمكن تحميلها من الرابط packetstormsecurity.org/groups/rhino9/legionv21.zip.

ETHEREAL

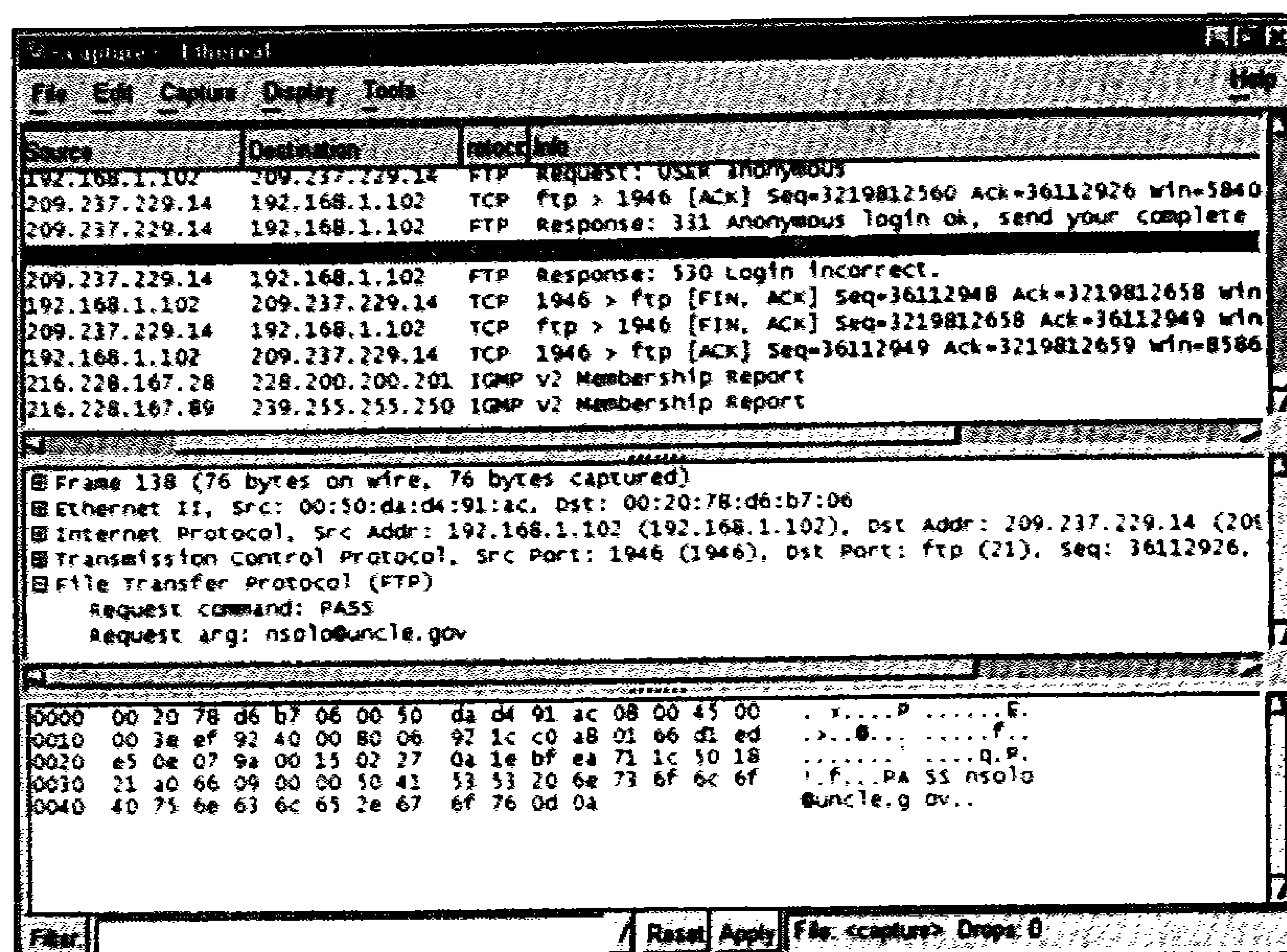
من أحد أشهر برامج sniffer للنظامين Windows وUnix، وهي أداة مجانية تسمى Ethereal (انظر الشكل 3-10). تمت برمجتها بالأصل من قبل Gerald Combs ومن ثم تحولت إلى مشروع مفتوح المصدر مع كثير من المساهمين، ويستخدمها مدراء الأنظمة كثيراً إلى جانب الجواسيس والمخرّبين من جميع أنحاء العالم.

يقوم البرنامج Ethereal بالتقاط حركة المرور الشبكية بشكل تفاعلي من شبكات Ethernet، Token-Ring، وشبكات أخرى بالإضافة إلى قراءة ملفات التقاط من برامج sniffer أخرى (تستطيع إجرائيات تحليل البروتوكولات إعادة بناء البيانات من أكثر من 340 بروتوكول مختلف). وهذا ملائم إذا كنت تريد تثبيت برنامج sniffer ذا حزمة صغيرة ومن ثم العودة لاحقاً لتفحص البيانات التي تم التقاطها. تتمتع الأداة Ethereal بإمكانيات ترشيح واسعة وخيار "متابعة مسار TCP (Follow TCP Stream)" لمراجعة دفق البيانات الكامل للجلسة.

يجب على كل جاسوس مهتم بالتنصت على الشبكة أن يمتلك الأداة Ethereal. لتحميل الأداة وللحصول على مزيد من المعلومات عنها، اتبع الرابط www.ethereal.com.

برامج sniffer أخرى

مع أن برنامج Ethereal وبرامج sniffer التجارية الأخرى مناسبة للتجسس وأغراض إدارة النظام الشرعية، لكن توجد أيضاً بعض برامج sniffer الأخرى والتي تم تصميمها خصيصاً للتجسس، ومن ضمنها ما يلي:



الشكل (10-3) الأداة Ethereal وهي تقوم بالتقاط حركة مرور الشبكة من جلسة FTP ومن ضمنها اسم حساب المستخدم وكلمة المرور.

- **Dsniff**: وهو برنامج sniffer لكلمات المرور مبرمج من قبل Dug Song والذي صُمم بالأصل للنظام Unix. يقوم البرنامج بدلاً من التقاط وعرض حركة المرور ضمن الشبكة، بإظهار أسماء الحسابات وكلمات المرور الملتقطة من البروتوكولات FTP، Telnet، HTTP، POP، NNTP، IMAP، IRC، AIM، Microsoft SMB، ومجموعة أخرى من بروتوكولات المصادقة. أصدر Mike Davis نسخة تعمل ضمن بيئة النظام Windows وهي متوفرة على الرابط www.datanerds.net/~mike/dsniff.html.
- **Ettercap**: وهو برنامج sniffer متعدد المنصات طوره Alberto Ornaghi وMarco Valleri، وهو مصمم لالتقاط البيانات على الشبكات المتبدلة باستخدام الانتحال عن طريق بروتوكول ARP. يمكنه مسح المعلومات على الشبكة وجمع كلمات المرور المستخدمة من قبل عدد من البروتوكولات. هذا البرنامج مجاني ويتوفر على الرابط http://ettercap.sourceforge.net.
- **Cain & Abel**: وهي أداة مذهلة لسكين الجيش السويسري والتي تقوم باعتراض البيانات على الشبكات المتبدلة واختراق عدد من كلمات المرور المشفرة التي تصادفها. مطور هذا البرنامج الخدمي هو Massimiliano Montoro، ويتوفر على الرابط www.oxid.it.

الإجراءات المضادة

يوجد عدد كبير من الإجراءات المضادة التي يمكنك استخدامها لتقوية نظامك ضد جواسيس الشبكة. كما تساعد هذه الدفاعات أيضاً على حمايتك من المهاجمات الشبكية التي يشنها المخرّبون، الذين يشكّلون تهديداً حيوياً نتيجة لأعدادهم المطلقة والأعداد الكبيرة لأدوات التخريب المتوفرة بسهولة على الإنترنت.

تتضمن بعض إجراءات الدفاع استخدام أدوات الهجوم نفسها التي يمكن أن يستخدمها الجاسوس ضدك (أي مواجهة النار بالنار)، لذلك سوف تملك فهماً أفضل لمساوئ نظامك. تتضمن الفقرة التالية الإجراءات المضادة الأساسية التي يجب اعتبارها أثناء مواجهة المتنصتين على الشبكة.

تطبيق تحديثات نظام التشغيل والتطبيقات

تأكد من تثبيت الترميمات الأمنية الحالية لكل من النظام Windows، مستعرض الإنترنت Internet Explorer، Outlook، منتجات Microsoft Office، وأية برمجيات تتصل بالإنترنت. (يستعرض الفصل الرابع عدة طرق لتحديث نظام التشغيل Windows والترميمات الأمنية البرمجية الأخرى لشركة Microsoft).

بسبب معاناة بعض التطبيقات مثل Outlook، Outlook Express، و Internet Explorer، من الثغرات الأمنية الكثيرة، يجب أن تستبدل عميل البريد الإلكتروني ومستعرض الإنترنت من شركة Microsoft بتطبيقات تابعة لفريق ثالث، وذلك إذا كنت جدياً حول موضوع الأمن. توجد الكثير من البدائل المجانية والرخيصة لهذه المنتجات من شركة Microsoft. (قد تستخدم بعض منتجات الطرف الثالث شيفرة من المستعرض Internet Explorer و Outlook عند تشغيلها، مما يعرّضها إلى نقاط الضعف نفسها التي يعاني منها مستعرض الإنترنت وعميل البريد الإلكتروني. لذلك إما عليك إجراء بعض البحث لضمان أن التطبيق لا يعتمد على الشيفرة غير الآمنة وإذا كان كذلك يجب أن تطبق الترميمات الأمنية لمستعرض الإنترنت Internet Explorer، وOutlook حتى لو لم تكن تستخدم منتجات شركة Microsoft). إلى جانب ذلك، يمكنك تثبيت نسخة رسومية لنظام التشغيل Linux حيث أصبح هذا النظام سهل الاستخدام للمستخدم العادي. وأيضاً تتوفر منتجات مثل Open Office لكلا النظامين Linux وWindows ، والتي تقدم بديلاً مجانياً لمجموعة البرامج المكتبية Microsoft Office. (هذا لا يعني أن النظام Linux وتطبيقاته غير معرّضين للمهاجمات. حيث كلما زادت شعبية هذا النظام، توقّع اكتشاف ثغرات أمنية أكثر في نظام التشغيل وتطبيقاته المرتبطة به. وهذا ارتباط إيجابي بين الشعبية ونقاط الضعف المكتشفة).

استخدام أنظمة كشف اختراق الشبكات IDS (Intrusion Detection Systems)

نظام كشف اختراق الشبكات IDS هو برنامج خدمي برمجي والذي يبحث عن دلالات تشير إلى أنه تم اختراق شبكتك. يستمع نظام الكشف هذا إلى حركة المرور الشبكية ويحللها إلى نماذج قد تشير إلى وقوع هجوم. يفحص نظام كشف اختراق الشبكات المضيف سجلات الملقم باحثاً عن نماذج الهجوم وقد يدمج أيضاً خيارات تكامل الملفات لكشف ملفات النظام المعدّلة سرياً. بعد أن يتم التعرّف على نموذج الهجوم من سلسلة من مجموعات القوانين، يحذّر نظام كشف اختراق الشبكات مدير النظام من وقوع الهجوم.

من بعض المنتجات التجارية والمجانية لأنظمة كشف اختراق الشبكات المضيفة للنظام Windows ما يلي:

- **Snort**: أداة مجانية، شائعة جداً، مفتوحة المصدر، لكشف الاختراق. تم تطويرها بالأصل لأنظمة التشغيل من النمط Unix، ومن ثم تم إصدار نسخة للنظام Windows. ينجز البرنامج Snort تحليلاً في الزمن الحقيقي لحركة المرور في الشبكة وتسجيل الحزم على الشبكات ويمكنه كشف عدد من المهاجمات المختلفة والاختراقات، مثل أخطاء فيضان التخزين المؤقت، مسح المنافذ الخفي، مهاجمات CGI، اختراقات SMB، ومحاولات بصم نظام التشغيل. هذا البرنامج معقّد قليلاً ليثبّته مستخدم غير تقني، لكن توجد بعض الجولات التعليمية المفيدة لتثبيته في نظام التشغيل Windows. تتوفر هذه الأداة على الرابط www.snort.org.

- **BlackIce PC Protection**: يتجادل بعض خبراء الأمن حول فيما إذا كان البرنامج BlackIce (المسمى سابقاً BlackIce Defender) هو بشكل أساسي نظام لكشف اختراق الشبكات IDS أو جدار ناري Firewall. يقدّم هذا المنتج الرائد أمنياً عدداً من الميزات الفعالة للمستخدم ذو مستوى متوسط وذو مستوى متقدم. تبلغ تكلفة الإصدار الوحيد للحاسب الشخصي 39.95 دولار أمريكي، وإصدار الملقم يصل إلى299.95 دولار أمريكي. لمزيد من المعلومات حول أداة BlackIce أو لتحميل إصدار تجريبي، اتبع الرابط www.iss.net.

- **Securepoint Intrusion Detection**: وهو نظام مجاني لكشف اختراق الشبكات، جديد نسبياً والذي يتعهد بالنجاح. تم تطوير هذا المنتج من قبل شركة أمنية ألمانية Securepoint ويمكن تحميله من الرابط www.securepoint.cc/en/products-sids.html.



يملك Robert Graham لائحة ممتازة بالأسئلة التي تتكرر باستمرار حول أنظمة كشف اختراق الشبكات، على الرابط:
www.robertgraham.com/pubs/network-intrusion-detection.html .

استخدام تطبيقات جدار الحماية

تقدّم تطبيقات جدار الحماية دفاعاً من المقتحمين بعملها كحاجز بين النظام الحاسبي والعالم الخارجي (عادة الإنترنت). تعمل تطبيقات جدار الحماية من خلال منع حزم بيانات محددة من الوصول إلى الحاسب بينما تسمح لأنواع أخرى من البيانات بالوصول إلى النظام. يمكنك تشبيه جدار الحماية بحارس لحركة المرور TCP/IP على شبكتك، مواجهاً الحزم بشكل مستمر لتعرّف نفسها هل هي صديق أم عدو، وذلك بناءً على مجموعة من القوانين قمت بتزويد جدار الحماية بها.

هناك تطبيقات جدار حماية برمجية وصلبة وأحياناً يتم استخدام كلا النوعين معاً. عموماً، تستخدم تطبيقات جدار الحماية ثلاثة أنواع من آليات الترشيح للحد من حركة مرور الشبكة، ومن ضمنها ما يلي:

- **ترشيح التطبيق Application filtering**: يُستخدم عادة في تطبيقات جدار الحماية البرمجية الشخصية، يسمح هذا النوع من الترشيح للاتصالات الشبكية الخارجية من التطبيقات الموثوقة وتحجب أو تحذّر المستخدم عند محاولة تطبيق غير موثوق تأسيس اتصال خارجي. وهذا الأمر مفيد لإيقاف تطبيقات حصان طروادة والبرامج التجسسية الأخرى التي تستطيع إرسال البيانات سرياً عبر شبكة الإنترنت.
- **ترشيح الحزمة Packet filtering**: وهو ببساطة السماح أو عدم السماح للحزم بالمرور بناءً على المعلومات الموجودة في ترويسة الحزمة. تقوم بتأسيس مجموعة من القوانين لقبول أو رفض الحزم بناءً على سماتها، مثل عنوان IP المصدر والوجهة، أرقام منافذ المصدر والوجهة، أو بروتوكول الشبكة.
- **تفحص الحزمة المتعلق بالحالة Stateful packet inspection (SPI)**: يتفحص تطبيق جدار الحماية عناوين IP للمصدر والوجهة، منافذ المصدر والوجهة، وأرقام التسلسل ليقرر فيما إذا كانت الحزم تنتمي إلى الاتصال المفتوح الحالي. وهذا يضمن أن جميع الاتصالات المؤسسة من قبل الحاسب الذي يعمل عليه تطبيق جدار الحماية وتحدث فقط مع الحواسب البعيدة المعروفة والموثوقة من خلال التفاعلات السابقة. تغلق تطبيقات جدار الحماية ذات المرشح SPI المنافذ حتى يتم طلب الاتصال إلى منفذ محدد، ويسّهل هذا الأمر التغلب على عملية مسح المنافذ.

يجب أن نشير إلى نقطة مهمة وهي أن تطبيقات جدار الحماية ليست سحرية ولا تزود طبقة حماية لا يمكن اختراقها بتاتاً. هناك عدد من الطرق لاختراق تطبيقات جدار الحماية، يعتمد الكثير منها على التصميم أو نقاط الضعف التي لم يتم ترميمها. (فعلى سبيل المثال، اتبع الرابط www.paoloiorio.it/fw.htm وتحقق من التطبيق FIREWAR الذي طوّره Paolo Iorio والذي يستطيع تعطيل الكثير من تطبيقات جدار الحماية الشخصية الشائعة عن بعد). تأكد من أنك تعلم جميع إمكانيات وقيود تطبيق جدار الحماية لديك، قبل أن تراهن بأمنك عليه.



يوجد عدد من الخدمات المجانية والتي تنجز اختراقات ومسح للمنافذ ضد حاسب ذو عنوان IP محدد بهدف اختبار تطبيق جدار الحماية المثبت على هذا الحاسب. من أحد المواقع التي توفر هذه الخدمات، موقع Steve Gibson وهو شائع جداً وموثوق ويمكنك الوصول إليه على الرابط www.grc.com/x/ne.dll?bh0bkyd2. كما يقدم الموقع Sygate خدمة شاملة لمسح المنافذ على الرابط http://scan.sygatetech.com.

تطبيقات جدار الحماية الصلبة

تكون وظائف جدار الحماية عادة مركبة داخلياً ضمن الموجّهات الشبكية Routers والمبدّلات الشبكية Switches والتي تعمل مثل عبّارة Gateway من الشبكة المحلية LAN إلى الشبكة الموسعة WAN تماماً مثل شبكة الإنترنت. ويتم التحكم بحركة المرور الداخلة والخارجة عبر مجموعة من القوانين يحددها المستخدم. تقوم بتحديد القوانين وتثبّت تطبيق جدار الحماية باستخدام بروتوكول Telnet أو مستعرض للاتصال بالجهاز ومن ثم تكوينه.

تشكّل كثير من الموجهّات Routers بروتوكول التكوين الديناميكي للمضيف DHCP وعملية ترجمة عنوان الشبكة NAT. يسند البروتوكول DHCP آلياً عناوين IP للحواسب المتصلة بالموجّه. هذه الميزة شائعة جداً بين مستخدمي الحواسب في المترل أو في الأعمال الصغيرة والذين يستخدمون الشبكات للمشاركة باتصال وحيد عريض النطاق. تخفي العملية NAT عناوين IP للحواسب خلف الموجّه، لذلك تبدو حركة المرور الخارجة من جميع الحواسب وكأنها تخرج من عنوان IP وحيد. يطلق بعض المصنّعين على المنتجات ذات العملية NAT اسم تطبيقات جدار الحماية، لكنها فعلياً ليست كذلك.

من الهام معرفة أنه لم يتم إنشاء تطبيقات جدار الحماية الصلبة بشكل متماثل. حيث لن يتمتع الموجّه Linksys الذي تبلغ تكلفته 100 دولار أمريكي والمصمم للاستخدام المترلي أو في الأعمال الصغيرة، بنفس المواصفات التي يتمتع بها موجّه Cisco المصمم للاستخدام داخل المؤسسات.

حيث تملك تطبيقات جدار الحماية للمؤسسات إمكانيات ترشيح وتسجيل حزم أكثر تعقيداً وتطوراً، وهي مجهّزة بصورة أفضل لتتحمل أحجاماً أكبر لحركة المرور الشبكية.

تطبيقات جدار الحماية البرمجية

مع انتشار الاتصالات ذات النطاق العريض للاستخدام المنزلي وللأعمال الصغيرة، زادت شعبية تطبيقات جدار الحماية البرمجية بشكل كبير خلال السنوات الماضية. يوجد نوعان من تطبيقات جدار الحماية البرمجية:

- **عبّارة Gateway**: تطبيق جدار الحماية العبّارة هو حاسب يتوضع بين شبكة الإنترنت والشبكة المحلية ومهمته مقصورة على تنفيذ تطبيق جدار الحماية أو برنامج موجّه. تحتل الحواسب القديمة 486 وحواسب Pentium التي تعمل على نظام التشغيل Linux وتنفّذ برمجيات أمنية مجانية دوراً شائعاً في هذا المجال. (إذا كنت مهتماً بهذا الموضوع، تحقق من الرابط /www.linux-firewall-tools.com/linux).
- **شخصي Personal**: يتم تثبيت تطبيق جدار حماية شخصي على حاسب مستقل ويعمل مثل حارس لحركة المرور الشبكية الداخلة والخارجة. تتضمن تطبيقات جدار الحماية الشائعة للنظام Windows Keiro، Norton، Sygate، و ZoneAlarm.

تسعى تطبيقات جدار الحماية الشخصية لتكون سهلة الاستخدام ولا تتطلب مهارات كبيرة لتثبيتها. يمكن استخدامها لوحدها أو مع تطبيق جدار حماية صلب لضمان الحالة التي قد يتم فيها اختراق أحد التطبيقين.

سبب آخر يدعو لاستخدام تطبيق جدار حماية شخصي هو أنها تدعم شيئاً لا تدعمه تطبيقات جدار الحماية الصلبة: الاتصالات الخارجة المُرشحة. حيث يمكن أن يشكّل تطبيق جدار الحماية ميزة مفيدة إذا تم تثبيت تطبيق حصان طروادة سرياً على حاسبك، لأنه يقوم بتحذيرك أن هناك تطبيق يحاول أن يؤسس اتصال خارجي إلى شبكة الإنترنت وإرسال البيانات. يمكنك اختيار التطبيقات الموثوقة، مثل مستعرض الويب، لكي لا يتم تحذيرك في كل مرة يقوم بها تطبيق موثوق بالاتصال بشبكة الإنترنت. (لا تزود تطبيقات جدار الحماية للنظام Windows XP (Internet Connection Firewall (ICF)) ترشيحاً للحزم الخارجة. لتجنب هذه السيئة يمكنك استخدام تطبيق جدار حماية تجاري أو مجاني من فريق ثالث لزيادة الأمن لديك).

يستطيع الجاسوس المحترف أن يستخدم مستعرض الإنترنت Internet Explorer لإرسال البيانات بشكل سري تحت إشراف تطبيق جدار الحماية. وإذا كنت مهتماً حول الأمن كثيراً، قد ترغب باستخدام مستعرض إنترنت مختلف مثل مستعرض Mozilla، Phoenix، أو Opera.

يملك معظم بائعو تطبيقات جدار الحماية الشخصية التجارية إصدارات مجانية لمنتجاتهم والمتوفرة للاستخدام الشخصي وتتمتع بمجموعة مخفضّة من الميزات (وهي خيار مثالي لحماية الحواسب المنزلية ضد هجوم شبكي).

إجراءات مضادة: مراقبة تطبيقات جدار الحماية

إذا كنت حريصاً حول أمنك، يجب أن تتحقق بصورة دورية من تسجيلات تطبيق جدار الحماية. يمكن أن تقدم المعلومات في السجلات علامات حول وجود أحد ما مهتم باختراق نظامك.

تتمتع الكثير من تطبيقات جدار الحماية الشائعة لكن غير الحديثة بإمكانيات تسجيل محدودة، ولا تقوم بعمل جيد في التقاط المعلومات حول الاختراقات ومحاولات الهجوم. توجد تطبيقات برمجية ترتبط بتطبيقات صلبة لتقديم معلومات أفضل حول النشاط الشبكي، ومن ضمنها الاختراقات والمهاجمات. هناك برنامجين خدميين شائعين:

- **WallWatcher:** أداة تسجيل مجانية لمنتجات Linksys، تتوفر على الرابط www.wallwatcher.com.
- **Kiwi Syslog Daemon:** أداة تعمل مع تطبيقات جدار الحماية وتقوم بتوليد خرج نظامي لسجلات النظام، تتوفر الإصدارات التجارية والمجانية على الرابط www.kiwisyslog.com.

يمكن أن تزودك هذه السجلات بإحصائيات مفصلة حول حركة المرور الشبكية لديك، ومن ضمنها الاتصالات المعادية.



للحصول على قائمة بائعي تطبيقات جدار الحماية، والموجهة بشكل أساسي إلى المؤسسات، تحقق من دليل شركة Computerworld Buyer's على الرابط www.computerworld.com/services/buyersguide/subcat/0،4846،KEY73_SUB16،00.html. ولمعلومات تفصيلية عن منتجات جدار الحماية للمكاتب والمنازل الصغيرة SOHO (Small Office Home Office) مع المواصفات والمراجعات، اتبع الرابط www.firewallguide.com.

تشغيل الشبكة الخاصة الافتراضية Virtual Private Network (VPN)

الشبكة الخاصة الافتراضية VPN هي شبكة خاصة تستخدم شبكة الإنترنت العامة بدلاً من خطوط شبكية محددة يتم استئجارها. تستطيع من خلال الشبكة الخاصة الافتراضية VPN أن تصل إلى الشبكة في منزلك أو مكتبك من أي مكان يوجد فيه اتصال بالإنترنت.

تعمل الشبكات الخاصة الافتراضية باستخدام عدد من البروتوكولات الخاصة مثل IPSec، L2TP، أو PPTP، بين حاسبين أو شبكتين متصلتين بالإنترنت. تسمى هذه العملية بالتغليف tunneling. يتم تشفير كل حزمة IP ومن ثم تغليفها داخل حزمة أخرى مع معلومات الترويسة والتي تسمح لها بالانتقال من نقطة إلى أخرى. عندما تصل الحزمة إلى الوجهة ، يزيل البرنامج الخاص بالشبكة الخاصة الافتراضية الترويسة، يفك تشفير الحزمة، ويوجهّها إلى وجهتها المطلوبة. تقدم الشبكات الخاصة الافتراضية طريقة آمنة للشبكات عبر الإنترنت دون تعريض بياناتك إلى الجواسيس المسلحين ببرامج sniffer على الشبكة.

يملك النظامان Windows 2000/XP دعماً داخلياً لإعداد اتصالات الشبكة الخاصة الافتراضية والتصرف كعملاء. توجد أيضاً الكثير من الحزم البرمجية التجارية والمجانية إلى جانب التجهيزات الصلبة من أجل إعداد الشبكات الخاصة الافتراضية. (أحد التطبيقات الشائعة والمفتوحة المصدر تسمى Stunnel، والذي يستخدم طبقة المقابس الآمنة Secure Sockets Layer لإعداد اتصالات آمنة بين الملقم والعميل. ولمزيد من المعلومات اتبع الرابط www.stunnel.org).

إجراءات مضادة: معرفة العدو

إحدى الطرق المتبعة لتتعرف فيما إذا كانت المهاجمات على نظامك تستهدفك بالتحديد أو هي جزء من سلسلة واسعة النطاق من المهاجمات التخريبية، هي تثبيت برنامج يحلل سجل تطبيق جدار الحماية ويرسله إلى ملقم مركزي يقوم بجمع وتحليل البيانات.

هناك عدد من الخدمات المجانية والتي تعالج بيانات سجل تطبيق جدار الحماية وتصرح عن أي محاولات اختراق إلى مزود خدمة الإنترنت الذي تولدت عنه هذه المحاولات. إذا رد مزود خدمة الإنترنت، يمكنك معرفة إذا تم اتخاذ أية تدابير ضد المهاجم المشتبه به. كما يمكنك أيضاً الإطلاع على معلومات حول عنوان IP ومعرفة إذا تم استخدامه للمسح أو لاختراق حواسب أخرى (أو إذا كنت هدفاً محدداً).

من أشهر هذه الخدمات، MyNetWatchman و Dshield، وهما مجانيتان. ولتحميل هذه الأدوات والحصول على معلومات أكثر، قم بزيارة مواقعها المرافقة:

- www.mynetwatchman.com.
- www.dshield.org.

تعتقد مزودات خدمة الإنترنت التي قامت بتطوير هذه الأدوات وإدارة هذه المواقع، أنه إذا استخدم معظم الناس العملاء فإن محاولات الهجوم غير المقصودة سوف تنخفض، وذلك لأن المهاجمون سوف يتحملون مسؤولية أفعالهم من قبل مزودات خدمة الإنترنت.



يشكّل الموقع VPN Labs مورداً ممتازاً للمزيد من المعلومات حول الشبكات الخاصة الافتراضية، لزيارة هذا الموقع اتبع الرابط www.vpnlabs.com.

مراقبة الاتصالات الشبكية

قد لا تحتاج أحياناً إلى جميع المعلومات التي يتيحها برنامج sniffer. ربما قد يراودك الفضول فقط حول احتمال وجود بعض البرامج التجسسية والتي ترسل المعلومات سرياً من حاسبك عبر شبكة الإنترنت. توجد عدة أدوات يمكن أن تستخدمها لمراقبة المنافذ على حاسبك والتي تتنصت وتستقبل البيانات.

أسهل طريقة للحصول على قائمة المنافذ المفتوحة حالياً هي طباعة الأمر التالي في موجّه سطر الأوامر: netstat –a.

السيئة الأساسية لهذا الأمر هو أنه لا يطلعك على البرنامج الذي يستخدم المنفذ. لكن لحسن الحظ، يوجد عدد من البرامج الخدمية سهلة الاستخدام للنظام Windows تزودك بمعلومات مفصلة أكثر حول المنفذ، ومن ضمنها ما يلي:

- **Inzider**: يعرض هذا البرنامج قائمة بالعمليات والمنافذ المستخدمة حالياً. هذا البرنامج مجاني ويتوفر على الرابط /ntsecurity.nu/toolbox/insider.
- **TCPView**: يعرض المنافذ المستخدمة حالياً أو التي أسست اتصالاً شبكياً. وهي مجانية وتتوفر على الرابط www.sysinternals.com.
- **TDImon**: أداة أخرى من شركة Sysinternals والتي تعرض معلومات حول بروتوكولات TCP وUDP في الزمن الحقيقي، ومن ضمنها العملية المتصلة بشبكة الإنترنت، منافذ المصدر والوجهة، وعناوين IP، ومعلومات شبكية أخرى.

استخدام برامج sniffer

ارتدي معطفك والعب دور الجاسوس بتنفيذ أحد برامج sniffer مثل Ethereal و Ettercap على شبكتك الخاصة للتعرف على نوعية البيانات التي يستطيع أن يكشفها المتطفل. قد تتفاجأ بالنتائج. وكلما تعلمت أكثر عن بروتوكولات الشبكة، كلما استطعت تفسير البيانات التي تعترضها بشكل أفضل، لكن ليس من الضروري أن تكون ساحراً شبكياً لتبحث عن كلمات المرور المرسلة بنص صريح، محتويات البريد الإلكتروني التي يمكن قراءتها بسهولة، أو معلومات أخرى من البيانات الحساسة التي تعبر الأسلاك.

مضبوط: Russel Filler ووكالة الفضاء الأمريكية NASA

ركب مقاول Russel Filler NASA البالغ من العمر 47 عاماً، في شهر تشرين الثاني (نوفمبر) عام 2002، طائرة Cessna ذات محرك وحيد مع مدرّب طيران لتجديد رخصة الطيران. حالما اعتدلت الطائرة على ارتفاع 9,000 قدم ونظر المدرّب في جهة معاكسة، فكّ Filler حزام مقعده وقفز من الطائرة. وُجدت جثته بعد يومين.

بدأت تظهر التفاصيل حول هذه القضية، ومن بينها حقيقة أنه كان سوف يتم اتهام Filler بسرقة حاسب محمول تابع لوكالة NASA اختفى من مركز الفضاء Johnson في نهاية شهر تشرين الأول (أكتوبر). لقد كانت وسائل الإعلام تغطي القضية من جميع جوانبها. وصرحّت أنه قاد جهاز تعقّب موجود في الحاسب المحمول السلطات إلى منزل Filler.

قبل انتحاره الجلي، أطلع Filler التحقيقات أنه رأى إعلاناً قديماً في متجر عن بيع حاسب محمول بقيمة 500 دولار أمريكي، وأخبرهم أنه كان يعلم بأنه مسروق، ولكنه لم يستطع تجاهله. لم تعر التحقيقات قصته أي اهتمام، وتم توجيه تهم ضده قبل موته.

صرحت السلطات بعدم وجود أية معلومات حساسة على الحاسب، لكنها لم تذكر أبداً ما الذي كان موجوداً داخل الحاسب المحمول والذي قادها إلى منزل Filler . هل كان جهاز تعقب GPS، بطاقة شبكية خاصة والتي كانت تتصل بالمنزل عبر الإنترنت، أو ربما مرسل راديو اتخذته السلطات مقراً لها؟ ربما، لكن من غير المحتمل.

هناك دليل يمكن طرحه وهو أن موظف وكالة NASA والذي أصدر الحاسب المحمول سابقاً، قام ببساطة بحفظ اسم حسابه وكلمة المرور مع إعدادات طلب الاتصال الهاتفي إلى أحد ملقمات وكالة NASA. وربما وجد Filler طلب الاتصال الهاتفي المخزن وقام بوصل الحاسب المحمول إلى خط الهاتف ومن ثم ضغط الزر "اتصال Connect". اتصّل الحاسب المحمول إلى الملقم، وبالتأكيد خزّن الملقم رقم هاتف المتصل، وبعد ذلك أرجعت السلطات رقم الهاتف إلى Filler. مع أنه من المحتمل أن تملك وكالة الفضاء الأمريكية NASA أجهزة إرشاد سرية ضمن حواسبها المحمولة، لكن على الأغلب أن Filler قد ارتكب خطأً نتج عنه سلسلة من الأحداث التي كلفته حياته.

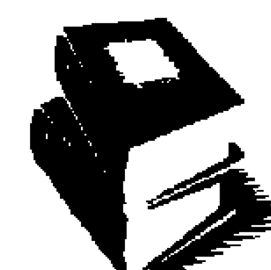
استخدام ماسحات المنافذ ونقاط الضعف

بشكل مشابه لاستخدام برامج sniffer ضد شبكتك الخاصة، يمكنك مسح منافذ الحواسب في شبكتك إلى جانب تنفيذ ماسحات لنقاط الضعف ضد هذه الحواسب. (لكن قبل أن تقوم بهذه العملية احصل على الإذن المناسب، لكي لا يتم ضبطك كجاسوس وينتهي بك الأمر في السجن). نأمل أن يضعك هذا التدريب في وضع أعلى من الجاسوس لكي تستطيع سد جميع

الثغرات التي سوف تجدها قبل أن يتم استغلالها. كما تساعدك هذه العملية في معرفة كيف تبدو عملية الهجوم والاقتحام وذلك عن طريق فحص نظام كشف اختراق الشبكات لديك وسجلات النظام بعد أن تكون قد نفذت مسحاً اختبارياً. يجب أن تنجز عمليات المسح الأمنية من داخل تطبيق جدار الحماية ومن خارجه، لأنه يمكن أن يتم شن الهجوم من كلا الجانبين. يجب إجراء عمليات المسح بشكل دوري لكشف الحواسب الجديدة في الشبكة، التغييرات البرمجية على الحواسب الموجودة، أو نقاط الضعف المكتشفة حديثاً (تأكد من تحديث برنامج مسح نقاط الضعف كلما قمت بتحديث برنامج مكافحة الفيروسات).

تشفير البريد الإلكتروني

يمكن أن تمنع الجواسيس من التنصت على بريدك الإلكتروني عن طريق تشفير رسائلك قبل أن ترسلها وتجعل الأشخاص الذين تتصل بهم يفعلون نفس الشيء. يعد برنامج PGP (Pretty Good Privacy) أداة ممتازة لتأمين البريد الإلكتروني نتيجة لشعبيته وتشفيره القوي.



لاسترجاع المعلومات حول برنامج PGP، راجع الفصل الرابع.

واحدة من مشاكل التشفير هي أنه إذا كنت مراقباً من قبل أحد ما، قد تجذب البيانات المشفرة الانتباه إلى نشاطاتك. حتى لو كان التشفير قانونياً، كما هو الأمر حالياً في الولايات المتحدة، توجد حالات عندما لا ترغب في إثارة شكوك الناس حول مراسلاتك. (من الواضح أنك إذا كنت تستخدم التشفير فإنه لديك شيء تخفيه، أليس هذا صحيحاً؟). إحدى طرق تجنب ذلك التدقيق الزائد هي استخدام Steganography، وهو إخفاء الرسائل ضمن نمط آخر من البيانات مثل صورة رقمية أو ملف MP3. تتضمن فقرة "الإجراءات المضادة" في الفصل الرابع معلومات أكثر حول هذه التقنية، كما تعرض بعض البرامج المصممة لإخفاء الرسائل. (مع انتشار الرسائل التي لا طائل منها SPAM، وهي طريقة اتصال سرية فعالة وذلك باستخدام بعض الكلمات السرية المرتبة سلفاً في رسالة إلكترونية إعلانية مجانية والتي تعدك بكثير من الأمور مثل جعلك غنياً، وغيرها. سوف يتعرّف المستخدم على هذه الرسالة بأنها سرية وليست رسالة SPAM، ويقوم بفك تشفير الكلمات المرتبة سابقاً. وإذا تم تنفيذ هذه العملية بنجاح، فلن يشك الشخص الذي يراقب البريد الإلكتروني في هذا).

تشفير الرسائل الفورية

لقد أصبحت المراسلة الفورية IM (Instant Messaging) شائعة جداً للأعمال والاستخدام الشخصي. حتى وقت قريب جداً، كان من الممكن مراقبة المحادثات التي تتم عبر المراسلة الفورية بسهولة باستخدام برامج sniffer، لأن جميع بروتوكولاتها كانت ترسل الرسائل بنص واضح. لكن توفرت مؤخراً بعض الوظائف الإضافية للمراسلة الفورية والتي تستخدم تشفيراً قوياً لحماية جلسات المراسلة من المتطفلين. فإذا كنت تعمل ضمن بيئة مشتركة واستخدمت المراسلة الفورية كجزء من عملك، عليك بالتأكيد استخدام التشفير للاتصالات الحساسة.

بعض الأمثلة التي تتضمن برامج تشفير مجانية أو رخيصة للمراسلة الفورية IM ما يلي:

- **Trillian**: منتج موحّد للمراسلة الفورية يدعم جميع بروتوكولاتها في واجهة مستخدم واحدة. يدعم كلا الإصدارين المجاني والتجاري (25 دولار أمريكي) التشفير القوي لمحادثات الخدمات AIM و ICQ. لمزيد من المعلومات اتبع الرابط www.trillian.cc.
- **SpyShield**: وظيفة إضافية مجانية من برنامج PGP للخدمتين MSN Messenger و Windows Messenger، وتتوفر على الرابط www.commandcode.com.
- **IIP (Invisible IRC Project)**: ويقدم تطبيق ملقم وكيل مجاني يؤمن وصولاً مشفراً مجهولاً إلى خدمة المحادثة IRC (Internet Relay Chat). يعمل الملقم الوكيل مع عميل نظامي لخدمة المحادثة IRC (مثل mIRC أو X-Chat) ويتصّل بعد ذلك إلى ملقمات IIP IRC خاصة لتزويد اتصالات آمنة. لمزيد من المعلومات عن هذا المشروع، اتبع الرابط www.invisiblenet.net/iip/index.php.

استخدام البروتوكولات الآمنة

كلما سنحت لك الفرصة لاستخدام بروتوكول آمن، يجب أن تستخدمه. مثلاً، بدلاً من استخدام البروتوكول Telnet استخدم البروتوكول SSH (Secure Shell)، وكذلك بدلاً من استخدام البروتوكول FTP استخدم البروتوكول SSH أو البروتوكول SCP (Secure Copy). إذا كان الملقم على الطرف الآخر من الاتصال يدعم هذه البروتوكولات، والكثير منها يفعل ذلك، سوف تكون كامل مناقلتك (ومن ضمنها اسم الحساب وكلمة المرور) مشفرة ولن تتم مراقبتها. توجد إصدارات تجارية ومجانية لعملاء وملقمات البروتوكول SSH. إذا كنت تستخدم البروتوكول SSH، تأكد من حيازتك على الإصدارات المحدثة منه، وخاصة إصدار الملقم وذلك بسبب إيجاد عدد من نقاط الضعف في أدوات مختلفة.



يملك John Fitzgibbon صفحة ويب شاملة مكرسة لاستخدام البرامج الخدمية المجانية SSH وSCP للنظام Windows وذلك لتأمين حركة مرور الشبكة. لزيارة موقعه اتبع الرابط www.jfitz.com/tips/ssh_for_windows.html.

لا تثق بالحواسب والشبكات "الغريبة"

هذا لا يعني أنه لا يمكنك استخدام حواسب Macintosh أو AppleTalk أبداً، لكن هذا يعني أنه عليك توخي الحذر من أي حاسب تتصل به إلى شبكة لا تثق بها ضمنياً أو لا تعرف بالتأكيد ما هو نوع الأمن الذي تم تنفيذه على ذلك الحاسب. مثلاً، قد تتضمن الحواسب العمومية مسجلات مفاتيح تعمل عليها أو تتم مراقبة حركة مرور الشبكة. إذا اضطررت إلى استخدام حاسب عمومي، تذكر أن تغير كلمة المرور لأية حسابات استخدمتها بوساطة حاسب غير موثوق حالما تصل إلى حاسب تثق به. تكون الشبكات العمومية أكثر أمناً نوعاً ما إذا كنت تستخدم حاسباً محمولاً آمناً، ، وخاصة إذا كنت تعتمد على استخدام بروتوكولات آمنة لأية اتصالات شبكية.

تقوية مشاركة الملفات لنظام التشغيل Windows

عندما يتعلق الأمر بمشاركة الملفات للنظام Windows، اتبع عدداً من الخطوات البسيطة والتي سوف تقوّي دفاعاتك ضد مهاجمات عائلة بروتوكولات NetBIOS، ومن بينها ما يلي:

- إذا لم تكن تستخدم مشاركة الملفات أو الطباعة، تأكد من أنها غير مفعّلة.
- قم بتعطيل بروتوكول TCP/IP لمشاركة الملفات أو الطباعة واستخدم البروتوكول IPX/SPX بدلاً منه. هذا يصعّب مهمة المقتحمين في الوصول إلى الموارد المشاركة عبر شبكة الإنترنت بشكل غير قانوني.
- استخدم دوماً كلمات مرور قوية، للحد من الوصول إلى البيانات المشاركة.
- قم بتقييد المشاركة إلى المجلد الذي يتضمن الملفات التي ترغب بمشاركتها. لا تشارك أبداً الدليل الجذر.
- قم بإعداد سماحيات المشاركة للمجلدات إلى أقل المستويات المطلوبة (مثلاً للقراءة فقط). لا تسمح أبداً بالوصول عن طريق الكتابة ما لم يكن هذا ضرورياً جداً.
- قم بالحد من الوصول إلى عناوين IP محددة، لأنه يمكن أن يتم انتحال أسماء ملقمات اسم المجال.

- أغلق منافذ عائلة بروتوكولات NetBIOS التي تستخدم بكثرة من قبل مشاركات النظام Windows على نطاق شبكتك عن طريق استخدام إما موجّه خارجي أو تطبيق جدار حماية على النطاق. المنافذ التي يجب أن تغلقها هي TCP 137-139، UDP 137-139، و TCP 445 و UDP.

استخدام ملقم بريد إلكتروني آمن

تقدّم أنظمة البريد الإلكتروني الشائعة مثل Microsoft Hotmail أو YahooMail حماية أصغرية من المتطفلين. يمكن أن يتم اعتراض الرسائل باستخدام برامج sniffer أو يتم استعراضها عند الملقم من قبل مدير النظام الذي يعمل لخدمة البريد الإلكتروني. إلى جانب ذلك، تملك الكثير من وكالات قوى القانون اتفاقيات مع مزودات خدمة الإنترنت ومزودات خدمة البريد الإلكتروني الرئيسة للوصول إلى البريد الإلكتروني. قبل أحداث 9/11 كان الأمر يتطلب أوامر من المحكمة، لكن حالياً أصبحت الكثير من مزودات خدمة الإنترنت متعاونة بصورة متزايدة مع قوى القانون في الاستجابة لطلبات الحصول على المعلومات.

قضية أمنية أخرى مع خدمات البريد الإلكتروني العمومية هي وثوقية النظام. فعلى سبيل المثال، تم اكتشاف خلل في خدمة Hotmail، في شهر آب (أغسطس) عام 1999. حيث يمكن إدخال اسم مستخدم معروف ضمن برنامج نصي بلغة HTML يتم كشف الصندوق الوارد للمستخدم بشكل كامل، ويمكن استعراض الرسائل، إرسالها، أو حذفها. تم نشر نقطة الضعف هذه بصورة واسعة قبل أن يتم إصلاحها، ومن الصعب تقدير كم عدد المستخدمين الذين تعرض بريدهم الإلكتروني للكشف.

إذا كنت من مستخدمي البريد الإلكتروني من مضيف ويب، استخدم بديلاً آمناً أكثر مثل Hushmail. حيث يستخدم Hushmail عدداً من تقنيات التشفير لمنع الجواسيس من التنصت على رسائلك. تبدأ باستخدام اتصالاً آمناً ذو طبقة المقابس الآمنة SLL إلى موقع الويب ذو خدمة البريد الإلكتروني، مما يمنع مراقبة البيانات بين حاسبك وملقم الويب. ومن ثم تدخل كلمة مرور لتصل إلى حساب البريد الإلكتروني. يقدم Hushmail مفتاحاً عمومياً بطول 2048 بت ذو نظام تشفير مبني على معيار OpenPGP لإرسال واستقبال الرسائل الإلكترونية المشفرة. (يستطيع مستخدمو Hushmail فقط تبادل الرسائل المشفرة بين بعضهم).

تم تصميم نظام Hushmail بحيث تخزن المفاتيح العمومية والخصوصية على ملقم ومن ثم تُشفر باستخدام عبارة مرور يختارها المستخدم. لخدمة Hushmail تم إصدار أمراً بتسليم نسخة من

المفاتيح أو الرسائل الإلكترونية المرسلة، ويمكن أن تمنح وكالة قوى قانون الإصدارات المشفرة فقط لأن الشركة لا تستطيع فك تشفير مفاتيح المستخدم وبريده الإلكتروني.

يمكنك التسجيل لحساب مجاني أساسي أو حساب اشتراك متقدم على الرابط www.hushmail.com.

استخدام البريد الإلكتروني المجهول Anonymous Remailers

البريد الإلكتروني المجهول Remailer هو ملقم يقوم بإرسال رسالة إلكترونية إلى أحد ما. على خلاف البريد الإلكتروني العادي، والذي سوف يترك عنوان IP للمصدر والزمن ضمن ترويسة الرسالة، ينتزع البريد الإلكتروني Remailer معلومات الترويسة والتي تحدد هوية المرسل.

لكي تستطيع استخدام البريد الإلكتروني Remailer قم بإرسال رسالة إلكترونية منسقة بشكل خاص إلى ملقم البريد الإلكتروني المجهول Remailer، مع تشفيرها باستخدام مفتاح PGP للبريد Remailer. عندما يستقبل الملقم الرسالة ، يقوم بفك تشفيرها تلقائياً، ومن ثم اعتماداً على تنسيق الرسالة يقوم بإرسالها إلى المستقبل. تتوفر ترويسات الرسالة فقط من البريد الإلكتروني Remailer، ولا توجد أية علامات عن هوية المرسل. إذا كان جاسوس ما يراقب بريدك الإلكتروني كل ما سوف يعرفه هو أنك قمت بإرسال رسالة إلى أحد ما عبر البريد الإلكتروني Remailer، لكن لن يعلم إلى من وجهت الرسالة. إذا كان أحد ما يتنصت على المستقبل، سيرى رسالة إلكترونية أتت من البريد الإلكتروني Remailer، لكن لن يعلم من هو مرسل هذه الرسالة.

تتضمن برامج البريد الإلكتروني Remailer جميع أنواع الميزات المتقدمة التي يمكن أن تستخدمها، بحسب مستوى ارتيابك. مثلاً، إذا أردت الاتصال بشكل آمن مع Natasha، سوف تقوم بتشفير الرسالة باستخدام برنامج PGP لديها قبل أن ترسله عبر البريد الإلكتروني Remailer. ومن ثم سوف تحشر تعليمات لتأخير الوقت ضمن التنسيق، بحيث ينتظر البريد الإلكتروني Remailer عدداً محدداً من الدقائق بعد أن يستلم الملقم الرسالة وقبل أن يرسلها إلى الوجهة. (إذا كان أحد ما يراقب البريد الإلكتروني Remailer، سوف يفترض أن الرسالة الصادرة مرتبطة بالرسالة الأخيرة الواردة، لكن التأخير في إرسالها سيشوش محاولات تعقب أثرها). وأخيراً من الممكن تقييد البريد الإلكتروني Remailer. هذا يعني أنه يمكنك إرسال الرسالة خلال سلسلة من ملقمات Remailer، في كل مرحلة يتم تشفير الرسالة بمفتاح PGP الخاص بالبريد الإلكتروني Remailer الموافق. بعد أن يتم تنسيق وتشفير الرسالة بصورة صحيحة سوف ترسلها إلى البريد الإلكتروني Remailer الأول، الذي يقوم بفك تشفير الرسالة ومن ثم إرسالها إلى البريد الإلكتروني Remailer الثاني في السلسلة وهكذا، حتى تصل الرسالة أخيراً إلى المستقبل.

يبدو كل هذا معقداً جداً وكان الأمر متعباً قليلاً للقيام بتشفير وتنسيق الرسالة بصورة صحيحة لتمر عبر ملقمات البريد الإلكتروني Remailer وذلك في بداية انطلاق هذا النوع من البريد الإلكتروني. لكن حالياً تتوفر برامج خدمية تجعل العملية أسهل بكثير.

البريد الإلكتروني المجهول Remailer مجاني ويتم تنفيذه عادة من قبل مؤيدي السرية مستخدمين الشيفرة المفتوحة المصدر لملقمات البريد الخاصة بهم. يوجد نوعان من البريد الإلكتروني Remailer: النوع الأول Cypherpunk والأكثر أمناً النوع الثاني Mixmaster، والذي يستخدم التقنيات المتطورة لتقديم أمن أكثر ضد حركة المرور. في بداية عام 2003، كان هناك خمسون ملقماً للبريد الإلكتروني Remailer حول العالم.

لمزيد من المعلومات حول البريد الإلكتروني المجهول، اطلع على الموارد التالية:

- www.sendfakemail.com/~raph/remailer-list.html. كثير من المعلومات حول أنواع مختلفة من البريد الإلكتروني المجهول Remailer. بعض الموارد والروابط قديمة، لكنه موقع جيد للمعلومات العامة.
- www.chez.com/frogadmin/. موقع ويب فرنسي مع إحصائيات حديثة حول البريد الإلكتروني Remailer وتحميلات للزبائن.



طوّر Joel McNamara أحد أدوات البريد الإلكتروني Remailer وPGP الأولى، وهي سهلة الاستخدام ومعتمدة على نظام التشغيل Windows، وتسمى Private Idaho (PI) عام 1995. لقد أصبحت قديمة بعض الشيء لكن يستخدمها بعض الأشخاص. تم إصدار هذه الأداة أخيراً مفتوحة المصدر، وتتوفر إصدارات محدثة أكثر من قبل مطورين آخرين. لمزيد من المعلومات حول الأداة Private Idaho و البريد الإلكتروني المجهولRemailer بشكل عام، اتبع الرابط www.eskimo.com/~joelm/pi.html.

استخدام ملقم وكيل ويب Web Proxy

يتوضع الملقم الوكيل بين حاسب العميل وملقم آخر ويعالج جميع الطلبات المرسلة بين العميل وملقم آخر. يتم إعداد ملقمات الوكيل للويب غالباً لتحسين أداء الشبكة عن طريق تخزين صفحات الويب المستخدمة بشكل متكرر وحفظ عرض الحزمة عن طريق تسليم المحتوى المحلي المخزن مقابل المحتوى المستلم عبر شبكة الإنترنت. كما يمكن أيضاً إعداد الملقم الوكيل لترشيح الطلبات. فعلى سبيل المثال، في الشبكة المحلية المشتركة، عندما يقوم موظف بالوصول إلى صفحة ويب يمر الطلب أولاً عبر ملقم وكيل، والذي قد يحجب مواقع ويب محددة.

بالإضافة إلى هذه الاستخدامات التقليدية للملقمات، توجد أيضاً أنواع من الملقم الوكيل مصممة خصيصاً للسرية. عادة، عندما يصل المستعرض إلى موقع ويب، يسجل ملقم الويب عنوان IP للعميل ومعلومات أخرى عنه. إذا كنت متصلاً عبر ملقم وكيل سوف يقوم ملقم الويب الوجهة بتسجيل المعلومات حول الملقم الوكيل وليس حولك.

يتم إرسال محتويات صفحة الويب إلى المستعرض أيضاً بشكل واضح، وأي شخص يراقب الاتصال يستطيع أن يستعرض هذه المحتويات. لكن هذا غير ممكن عند الوصول إلى مواقع تستخدم بروتوكول طبقة المقابس الآمنة SSL، لأنه يتم تشفير جميع البيانات. تشفّر بعض ملقمات الوكيل السرية مواقع الويب التي تمت زيارتها باستخدام طبقة المقابس الآمنة، سواء كان موقع الويب يدعمها أم لا. مثلاً، إذا قمت بزيارة موقع وكالة الاستخبارات المركزية الأمريكية cia.gov، سيقوم ملقم الوكيل بتشفير الصفحات المطلوبة باستخدام طبقة المقابس الآمنة SSL ويرسلها إلى مستعرضك حيث يفك تشفيرها لتُعرض. وأي شخص كان يراقب اتصالك الشبكي سيعلم فقط أنك كنت متصلاً إلى ملقم وكيل وتستقبل بيانات مشفرة. ولن يعرف أنك كنت تزور موقع CIA، وكجائزة لك، لن يسجل ملقم الويب الخاص بوكالة CIA عنوان IP الخاص بك كزائر.

إذا قررت استخدام ملقم وكيل لضمان أمن استعراض الإنترنت، عليك اعتبار النقاط التالية:

- أخيراً، يجب أن تثق بأي شخص ينفّذ الملقم الوكيل لأنه يستطيع مراقبة وتسجيل جميع الاتصالات.
- استخدم ملقم وكيل يدعم بروتوكول HTTPS (Hypertext Transfer Protocol Secure). وهو ببساطة أداة تنفيذية للبروتوكول HTTP والذي يستخدم طبقة SSL لتشفير البيانات.
- بالرغم من أنه يمكن تشفير المحتوى، إلا أن محددات مواقع المعلومات URLs والتي تظهر في مجلد المحفوظات للمستعرض لن تكون مشفرة. تقوم بعض الملقمات بمزج محدد موقع المعلومات لكي لا يستطيع المتطفل إظهار لائحة العناوين التي كنت تزورها.
- قد تكون عملية الاستعراض أبطأ بكثير، بحسب حمل الملقم الوكيل.
- يمكن إنجاز تحليل حركة المرور بناءً على كمية المعلومات التي تم تحديدها، مثلاً، قد تفترض كمية كبيرة من النشاطات الشبكية أنه تم تحميل ملفات ذات حجم كبير، مثل ملفات MP3 أو برمجيات قرصنة.

يوجد عدد من ملقمات الوكيل التجارية والمجانية والتي تساعدك على إخفاء نشاطات استعراض الإنترنت من المتطفلين. تحقق من دليل محرك البحث Google للملقمات المجانية للحصول

على مزيد من المعلومـــات وقوائم بالخدمـــات والملقمـــات الحالية. وتتوفر على الرابط
.http://directory.google.com/Top/Computers/Internet/Proxies/Free/

تلخيص

يستطيع الاتصال الشبكي تزويد الجاسوس بعدة طرق لكشف البيانات. حيث توضّح التقنيات التجسسية الموصوفة في هذا الفصل فيما يتعلق بالمهاجمات الشبكية المحتملة. سوف يستخدم الجاسوس المحترف طرقاً وأدوات معقدة للاستفادة من الاتصال الشبكي لتحقيق أهدافه.

إذا كنت تتعامل مع بياناتٍ حساسة، لا تستخف بأمن الشبكات أبداً. حيث من الهام جداً أن تقوم أنت أو أحد ما من منظمتك بتعلم نقاط الضعف الشبكية والبقاء على اتصال مستمر مع نقاط الضعف الجديدة، والترميمات البرمجية التي يمكن أن تظهر بشكل يومي.



التنصت على الشبكات اللاسلكية 802.11b

مقدمة إلى الشبكات اللاسلكية

تتزايد شعبية الشبكات المحلية اللاسلكية 802.11b WLANs (wireless local area networks 802.11b) بشكل كبير. تظهر الشبكات المحلية اللاسلكية في المؤسسات، المنازل، المطارات، الفنادق، المطاعم، والمقاهي. وفقاً لإحصائيات شركة Gartner Dataquest، فقد وصلت مبيعات أجهزة الشبكة اللاسلكية إلى أكثر من 26 مليون وحدة في عام 2003، مقارنة مع 15 مليون وحدة تم بيعها في عام 2002. ويُتوقع أن تستمر الزيادة في الأسواق حتى عام 2007. وكما توقعت شركة Gartner فقد استعمل قرابة خمسون بالمائة من مستخدمي الحواسب المحمولة الشبكات اللاسلكية بنهاية عام 2003.

تتميز الشبكات المحلية اللاسلكية WLANs بأنها رخيصة وسهلة التركيب (عندما تمر معك كلمة WLAN في هذا الفصل، فهي تشير إلى شبكة 802.11b). كما أنها تسهّل حياة الجاسوس الحاسبي كثيراً. عندما تمزج بين الأمن الضعيف للبرتوكولات، إعدادات التجهيزات الافتراضية وغير الآمنة، والمستخدمين غير المطلعين جيداً مع تجهيزات اعتراض غير مكلفة وبرمجيات تنصت سهلة الاستخدام، فستحصل على وصفة مثالية للتجسس.

قبل أن نتحدث حول كيفية قيام الجاسوس باختراق شبكة WLAN، سوف نعرض ملخصاً سريعاً وبسيطاً حول بعض أساسيات الشبكة اللاسلكية. إذا كانت لديك معلومات مسبقة حول شبكة 802.11b، يمكنك تجاوز هذه الفقرة والانتقال مباشرة إلى أساليب الجواسيس.

تاريخ الشبكة اللاسلكية

تم تأسيس المعيار 802.11 عام 1997 من قبل معهد المهندسين الإلكترونيين والكهربائيين IEEE، واضعاً الأساس للشبكات اللاسلكية الحالية. 802.11b هو أحد تغيرات المعيار ويُعرف أيضاً باسم Wi-Fi، أو Wireless Ethernet (شبكة Ethernet اللاسلكية). منذ أن أُطلقت المنتجات الأولى للمعيار 802.11b عام 1999، أصبح المعيار 802.11b هو المعيار الأشهر والأكثر استخداماً للشبكات اللاسلكية.

يتم نقل البيانات ضمن شبكة 802.11b عبر الموجات الراديوية بسرعات تصل إلى 11Mbps. تتصل أجهزة الشبكة مع بعضها باستخدام المجال الترددي 2.4GHz مع 15 قناة (القنوات الإحدى عشرة الأولى مستخدمة في الولايات المتحدة ومبنية على تخصيص الطيف الترددي الراديوي التابع لهيئة الاتصالات الفدرالية في الولايات المتحدة FCC). يملك الحاسب ضمن شبكة WLAN بطاقة واجهة شبكة لاسلكية NIC (Network Interface Card) والتي تتضمن مرسل/مستقبل. يمكن أن تكون بطاقة واجهة الشبكة بطاقة شبكة ضمن حاسب محمول، بطاقة تمديد تقليدية في الحاسب الشخصي المكتبي، أو جهاز يتصل بالحاسب من خلال منفذ USB.

تملك معظم الشبكات المحلية اللاسلكية WLANs، إضافة إلى بطاقات واجهة الشبكة NICs، جهازاً يدعى نقطة الوصول AP (Access Point)، أو محطة القاعدة، وهو عبارة عن مرسل/مستقبل يتصل مباشرة إلى شبكة الإنترنت أو إلى مجمّع أو موجّه الشبكة. دور نقطة الوصول يماثل الجسر بين الشبكة السلكية والحواسب ذات بطاقات واجهة الشبكة اللاسلكية. ومع زيادة شعبية الشبكات المحلية اللاسلكية WLANs، بدأ المصنّعون يعرضون أيضاً موجّهات لاسلكية.

تتضمن كل من بطاقات الشبكة NIC ونقاط الوصول AP هوائيات مدمجة بداخلها لإرسال واستقبال الموجات الراديوية. يتراوح المجال الداخلي للأجهزة اللاسلكية بين 50 و150 قدم، ويحوي البعض هوائيات خارجية لتمديد تغطيتها.

الميزة الأساسية للشبكة اللاسلكية WLAN هي إمكانية تركيبها بسهولة وبسرعة دون امتلاك معرفة كاملة بتركيب الأسلاك أو التشبيك. يمكن إعداد شبكة صغيرة بسهولة مقابل عدة مئات من الدولارات، ببساطة عن طريق توصيل بعض الأجهزة.

لكن ما لم يتم تأمين الشبكات المحلية اللاسلكية WLANs، يمكن أن يتم التجسس عليها بسهولة دون أن يلاحظ ذلك مدير الشبكة حيث يمكن أن يجلس الجاسوس في سيارته قرب مقهى، يشرب القهوة، ويقوم بشكل سري يقوم بالتقاط حزم البيانات من شبكة محلية WLAN الموجودة في الشارع المجاور.

أساليب الجواسيس

حان الوقت لتفكر مثل الجاسوس ثانية. هذه المرة أنت خبير بالإجراءات المضادة للمراقبة التقنية TSCM أو ما يسمى Sweeper. تكسب رزقك عن طريق اكتشاف أجهزة المراقبة المرئية والصوتية لزبائنك، ومن بينهم رجال السياسة، مدراء أعمال تنفيذيون، وأشخاص آخرون يعتقدون أن خصوصيتهم قد تتعرض للكشف إلكترونياً. دخلك جيد لكنك تحتاج إلى توسيع خدماتك للبقاء في حقل المنافسة. تعلم أن أمن الحواسب هو الاتجاه المنطقي وبما أنك كنت تتعامل مع أجهزة المراقبة اللاسلكية لسنوات طويلة، تقرر أن تصل إلى حد معين في مجال الشبكات اللاسلكية أولاً. الطريقة الجيدة لتحقيق ذلك هي النظر إلى الموضوع من وجهة نظر الجاسوس.

السؤال الأول الذي قد يخطر لك هو السبب الذي يجعل الجاسوس يخترق الشبكة اللاسلكية WLAN. فكر بالموضوع لدقيقة أو اثنتين، ومن ثم تحقق إذا كان جوابك يطابق الأمور التالية:

- الوصول إلى الملفات والمعلومات المخزنة في مكان ما ضمن الشبكة.
- البحث عن حسابات المستخدمين وكلمات المرور.
- تثبيت تطبيقات حصان طروادة أو برمجيات أخرى سرياً على حواسب الشبكة.
- استخدام الشبكة اللاسلكية WLAN كنقطة انطلاق لشن المهاجمات على أهداف أخرى.

بالرغم من أن التقنية التحتية للشبكة اللاسلكية WLAN معقدة بعض الشيء، إلا أن طرق كشف الشبكة واختراقها بسيطة نسبياً. في معظم الحالات، لا تحتاج إلى خبرة كبيرة في مجال الشبكات أو شهادات مصدقة لتحديد الوصول إلى شبكة لاسلكية. حيث من الممكن كثيراً أن يكون مراهق ما جالس في سيارته ويقوم بهذا حالياً.

بما أن التقنية اللاسلكية غير ناضجة تماماً، ولا يدرك معظم المستخدمون أخطار التجسس التي يواجهونها عندما يركّبون شبكة لاسلكية. لذلك دعونا ندقق في بعض نقاط الضعف، التي يمكن أن تستغلها وبعض أدوات التجسس التي يمكن أن تستخدمها.

استغلال نقاط الضعف

قبل أن نبدأ من المهم معرفة أنه لم يتم تصميم المعيار 802.11b لتزويد الأمن على المستوى الصناعي. ويوجد عدد من المساوئ المتأصلة في البروتوكول والتي يمكن أن يستغلها الجاسوس.

شبكة SSIDS

تستخدم الشبكة اللاسلكية 802.11b معرفات المجموعة الخدمية (service set identifiers) SSIDs كجزء من أمنها، وهي اسم لشبكة لاسلكية محددة. وتشبه اسم مجموعة العمل ضمن شبكة Microsoft. لكي يرتبط الحاسب اللاسلكي بشبكة، يجب إعداد بطاقة الشبكة NIC لنفس قيمة SSID مثل نقطة الوصول AP. ويوجد عدد من المساوئ التصميمية والتنفيذية في هذا النموذج والتي يمكن أن يستغلها الجاسوس.

السيئة الأولى هي استخدام المصنّعين أرقام SSID الافتراضية لنقاط الوصول APs. مثلاً، إذا قمت بشراء نقطة وصول من شركة Cisco، فإن قيمة SSID الافتراضية لها هي tsunami. وفيما يلي جدول لقيم SSID الافتراضية من المصنّع مباشرة:

الجدول (11-1) قيم SSID الافتراضية لنقاط الوصول الشائعة APs

SSID	المصنّع
Tsunami، WaveLan Network	Cisco
101، comcomcom	3Com
WLAN	Dlink
Default SSID	Bay
WLAN	Addtron
101، 195، intel، xlan	Intel
Linksys، Wireless	Linksys
Wireless	Netgear
WLAN، BRIDGE	SMC
RoamAbout Default Network Name	Lucent/Cabletron
Compaq	Compaq

إذا تطابقت بطاقة الشبكة لديك مع رقم SSID لنقطة الوصول و لم تتواجد أية إجراءات أمنية أخرى في الشبكة، سوف يرتبط حاسبك بشبكة الهدف. بعد أن تتصل بالشبكة يمكن أن تستخدم أدوات الاختراق المفضلة لديك.

إن إدخال قيمة SSID الافتراضية بالتجريب أمر متعب، وماذا يحصل لو قام مدير الشبكة بتغيير الاسم الافتراضي؟

تبث نقطة الوصول باستمرار قيمة SSID عدة مرات في الدقيقة بما يسمى إطار الإنذار Beacon Frame. وكل ما يحتاجه الجاسوس هو حاسب محمول يحوي بطاقة شبكة لاسلكية وبرمجيات مناسبة، ويمكنه أن يخمن قيمة SSID للشبكة اللاسلكية WLAN ومن ثم تحديدها في برنامج الإعداد لبطاقة الشبكة لديه وأن يحاول الارتباط بالشبكة.

السرية المكافئة للسرية السلكية WEP (Wired Equivalent Privacy)

لقد واجهت بصفتك خبير تقني عدداً من أجهزة المراقبة عالية المستوى والتي زرعتها الحكومة. حيث بدلاً من إرسال إشارة راديوية تماثلية، قاموا بإرسال إشارة رقمية مشفرة. لقد سمعت أن الشبكة اللاسلكية WLAN تدعم التشفير، لذا هل يحمي التشفير الشبكة من التنصت والمراقبة؟

يجب التغلب على شيء أصعب في شبكة 802.11b، وهو ما يسمى السرية المكافئة للسرية السلكية WEP (Wired Equivalent Privacy)، وغالباً تسمى WEP. لقد كان مصممو الشبكة 802.11b يعلمون أنه يمكن اعتراض إشارات الراديو بسهولة، لذلك فإن الهدف من تقنية WEP هو تحقيق الأمن القريب من أمن الشبكات السلكية التقليدية من خلال استخدام التشفير.

تستخدم تقنية WEP تشفيراً دفقياً لخوارزمية RC4 بطول 64 بت لتشفير البيانات. يتم توليد مفتاح الشيفرة من قيمة أولية تقوم بدمج مفتاح WEP محدد من قبل المستخدم بطول 40 بت وقيمة شعاع التهيئة IV بطول 24 بت. سبب صغر مفتاح WEP هو أن الطول 40 بت هو طول المفتاح الأعظمي الذي سمحت به الولايات المتحدة. أنظمة التصدير للتشفير في ذلك الوقت. يتكون مفتاح WEP من سلسلة من عشرة محارف ست عشرية أو سلسلة من خمسة محارف نصية ASCII.

بسبب صغر المفتاح، يمكن أن يتم اختراق التشفير RC4 باستخدام هجوم القوة العمياء في غضون بضعة أيام، كما يستخدم كثير من مصنّعي الشبكات 802.11b تشفير RC4 باستخدام مفتاح بطول 128 بت. مع أنه ليس جزءاً من مواصفات البروتوكول، أصبح هذا المستوى الأقوى من التشفير شائعاً جداً، كما يتم استخدام شعاع تهيئة ذو مفتاح بطول 24 بت مع

مفتاح WEP بطول 104 بت. في هذه الحالة يتألف المفتاح من سلسلة من ستة عشر محارف ست عشرية أو سلسلة من ثلاثة عشر محارف نصية ASCII.

يوجد أيضاً مخطط مصادقة اختياري في البروتوكول يستفيد من آلية تشفير WEP. حيث أن مصادقة المفتاح المشترك هي نظام بدائي، مؤتمت، مشفر، حيث يتم توليد البيانات وإرسالها إلى العميل، يشفّر العميل البيانات ويعيد إرسالها، ومن ثم يتم فك تشفير الرد والتحقق منه ليتم التأكد أنها البيانات الأصلية التي تم إرسالها.

عندما يتم استخدام تقنية WEP في شبكة لاسلكية، يجب أن تستخدم نقاط الوصول وبطاقات الشبكة نفس مفاتيح WEP. تسمح هذه العملية أن يتم تشفير وفك تشفير البيانات بنجاح إلى جانب مصادقة الزبائن لكي يرتبطوا بالشبكة، كما يمكن استخدام ما يصل إلى أربعة مفاتيح بطول 40 بت (أو مفتاح واحد بطول 104 بت) بنفس الوقت.

لكن يوجد عدد من المساوئ المرتبطة بتقنية WEP. الأولى وهي ليست خطأ البروتوكول أن معظم المصنّعين لا يفعّلون خيار WEP في منتجاتهم. وعندما لا يتم استخدام هذه التقنية يمكن استعراض حزم البيانات بنص صريح من خلال برنامج sniffer (والذي سوف نناقشه في فقرة "أدوات التنصت على الشبكة اللاسلكية").

والسيئة الثانية هي أنه حتى لو تم تفعيل تقنية WEP سوف يتم تشفير حزم البيانات فقط، أما الحزم المستقلة والتي تتضمن معلومات الإدارة، مثل عنوان المصدر والوجهة، قيمة SSID، وعنوان MAC فيتم إرسالها كلها بالنص الصريح. وبالتالي حتى لو لم تستطع قراءة حزم البيانات المشفرة باستخدام برنامج sniffer، ما زال بإمكانك اكتشاف كمية هامة من المعلومات حول الشبكة عن طريق حزم الإدارة.

والسيئة الأخيرة الأعظم تتعلق بتنفيذ التشفير نفسه. عندما تبدأ تقنية حاسبية بالانتشار، يبدأ أمنها تلقي الكثير من التفحص والتدقيق، ولم تكن تقنية WEP استثناءً للقاعدة. حيث أدت سلسلة الأبحاث التي أجريت في النصف الأول من عام 2001 إلى تبديد الأوهام حول أمن شبكات 802.11b. ومن جهتها أدت هذه الأبحاث إلى تطوير عدد من الأدوات البرمجية التي تستطيع اختراق شبكة لاسلكية تحوي تقنية WEP.

حيث يستطيع أي شخص دون أن يتمتع بخبرة تقنية كبيرة اختراق تقنية WEP باستخدام أجهزة غير مكلفة وبرمجيات مجانية.

أساليب: هجوم WEP

يعشق الجواسيس الجزء الأكاديمي من عالم الحواسب: حيث يتطلع الأشخاص الفضوليون إلى تكوين ثغرة في النظام الأمني المفترض أنه مصمم جيداً. وقد خضعت شبكات 802.11b إلى عملية استنزاف أمنية في عام 2001 وقد تغير مظهرها الجميل بعد ذلك كثيراً.

كانون الثاني (يناير) عام 2001 – نشرت مجموعة أمن الإنترنت والتطبيقات والمصادقة والتشفير (ISSAC) في جامعة كاليفورنيا مقالة تشرح نقاط ضعف شعاع التهيئة IV والمجموع التدقيقي لخوارزمية RC4. لقد كانت اللجنة الفرعية لشبكات 802.11b تعلم مسبقاً هذه المساوئ، وسوف يتم إجراء تغييرات في الإصدارات القادمة. وتم استبعاد احتمال المهاجمات بصفتها تهديداً قوياً لأنها كانت تتطلب كمية كبيرة من القدرة الحسابية.

آذار (مارس) عام 2001 – نشر الباحثون في جامعة Maryland مقالة تستكشف نقاط الضعف لعملية إرسال بيانات إدارية غير مشفرة ومساوئ مصادقة المفتاح المشترك (التي ناقشناها)

تموز (يوليو) عام 2001 – كشف الباحثون Fluhrer، Mantin، و Shamir أنه يمكن تحديد قيمة مفتاح WEP من خلال معرفة قيمة شعاع التهيئة غير المشفرة وطريقة فك تشفير البايتات الأولى من البيانات. وبعد مضي شهر. عرض فريق من جامعة Rice و AT&T بنجاح تجربة هجوم عملي مبني على الورق وقاموا بكشف مفاتيح WEP في غضون ساعات باستخدام تجهيزات جاهزة.

بالرغم من أن الباحثين من جامعات Rice و AT&T لم ينشروا الشيفرة التي استخدموها في الهجوم علناً، لكن تم إفشاء السر بدون قصد. حيث نُشرت بعد عدة أشهر سلسلة من الأدوات عبر شبكة الإنترنت أعطت أي شخص القدرة على كشف شبكة لاسلكية. قم ببساطة بمعرفة مفتاح WEP، استخدم المفتاح المكتشف لبطاقة الشبكة اللاسلكية لديك، ويمكنك الاستماع إلى البيانات أو (تنفيذ أية إجراءات أمنية أخرى) المرتبطة بالشبكة.

انتبه دوماً إلى الأبحاث الحالية. كلما زاد عدد المساوئ ونقاط الضعف، كلما كان أفضل لك.

قوائم الوصول إلى عناصر التحكم بالوصول إلى الوسائط MAC (Media Access Control)

تملك جميع بطاقات الشبكة NICs ونقاط الوصول APs اللاسلكية عنوان التحكم بالوصول إلى الوسائط (MAC). وهو رقم فريد ذو تشفير ثابت يخصص للأجهزة التي تشكل عقد الشبكة. حيث تتم طباعة عنوان MAC، الذي في البرمجيات الثابتة للجهاز، في مكان ما على السطح الخارجي للمنتج. وتحدد الأرقام الستة الأولى لعنوان MAC المصنّع، والأرقام الستة المتبقية هي معرّف فريد للمنتج.

يتم تمرير عناوين MAC للمصدر والوجهة، بشكل مشابه لعناوين IP، جيئة وذهاباً بين الأجهزة التي تتصل ببعضها.

توجد ميزة أمنية أخرى لشبكات 802.11b وهي قائمة الوصول إلى عنوان MAC، وهي قائمة بالأجهزة المخوّلة التي تستطيع الوصول إلى الشبكة عبر نقطة الوصول AP. فإذا حاول حاسب محمول ذو بطاقة شبكة لاسلكية الارتباط بالشبكة، و لم يكن عنوان MAC لبطاقة الشبكة ضمن قائمة نقاط الوصول المخولة، سوف يتم منع الحاسب المحمول من الانضمام إلى الشبكة.

بالرغم من أنه قد تبدو لك عملية ترشيح عنوان MAC إجراءاً أمنياً معقولاً، لكنه مع ذلك يعاني من عدة مساوئ هي:

- أولاً، إذا استطعت أن تصل إلى الحاسب فيزيائياً أو فقط إلى بطاقة الشبكة، سوف تسمح لك نقطة الوصول آلياً بالانضمام إلى الشبكة.
- ثانياً، حتى لو لم تملك الوصول الفيزيائي، يمكنك دائماً أن تتنكر كعميل مخوّل لأنه يمكن انتحال عناوين MAC بسهولة. وبالرغم من أن عنوان MAC المعطى من المصنّع هو بث من الجهاز نفسه، لكن يمكن تجاوز هذه القيمة عن طريق نظام التشغيل وبرمجيات أخرى.

بالنظر إلى هذا من وجهة نظر الجاسوس، لنفترض أنك تتنصت على شبكة غير مشفرة وتعرف عناوين MAC وقيم SSID التي يتم استخدامها. فتقوم بإعداد قيمة SSID للهدف على بطاقة الشبكة لديك، لكنك لا تزال لا تستطيع الانضمام إلى الشبكة. خطوتك التالية هي أن تحاول تغيير عنوان MAC لديك إلى أحد قيم MAC التي تستخدمها الشبكة.

أساليب: انتحال عناوين MAC في نظام التشغيل Windows

تخزن أنظمة التشغيل Windows 2000/XP عناوين MAC لبطاقات الشبكة ضمن تسجيل النظام Registry. وإذا أردت كجاسوس أن تظهر بعنوان MAC مختلف، اتبع الخطوات التالية:

قم بتخزين نسخة احتياطية من التسجيل Registry.

ابحث عن برنامج التشغيل لبطاقة الشبكة ضمن:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE103181}.

ابحث ضمن المفاتيح الفرعية لتجد بطاقة الشبكة اللاسلكية.

قم بتغيير قيمة عنوان الشبكة إلى عنوان MAC من اختيارك. نموذجياً، يجب أن يوافق القسم الأول من العنوان رقم تعريف المصنّع لبطاقة الشبكة ليتم الارتباط بشكل صحيح بعنوان IP (أي تأسيس قناة اتصال بين برنامج تشغيل البروتوكول، مثل TCP/IP وبطاقة الشبكة NIC). مثلاً، إذا كانت بطاقة الشبكة لديك من نوع Lucent وحاولت تغيير قيمة عنوان MAC إلى قيمة جديدة قسمها الأول هو رقم التعريف الخاص بالمصنّع Linksys، غالباً سوف يفشل الارتباط. ويمكنك أن تجد لائحة كاملة لعناوين MAC لجميع المصنّعين، على الرابط http://standards.ieee.org/regauth/oui/index.shtml.

قم بتنفيذ الأمر IPCONFIG /ALL لمعرفة إذا تم تحديد العنوان الجديد.

توجد بعض أنواع البطاقات الشبكية اللاسلكية التي يمكن تغييرها بسهولة مثل ORiNOCO و Silver. ويمكن إدخال عنوان MAC جديد الذي يستبدل العنوان القديم الذي جاء من قبل المصنّع عن طريق استخدام برمجيات إدارية. وهناك بعض الأسباب الإدارية الشرعية لتطبيق هذه الميزة، مثلاً تحتاج بعض أنظمة التشغيل الشبكية أن يتم تعريف كل جهاز بعنوان MAC محلي، أي أنها ليست فقط للجواسيس. وإذا وجدت هذا الأمر معقداً جداً، توجد أداة سطر الأوامر اسمها BWMACHAK طورها قرصان لاسلكي اسمه BlackWare، وتقوم بتغيير عنوان MAC بسرعة.

الأمواج الراديوية Radio Waves

لقد وجدتَ خلال مهنتك عدداً من أجهزة المراقبة التي ترسل إشارات ضمن المجال 398 إلى 399.5 MHz. تبيع الكثير من متاجر الجواسيس هذه الأجهزة القديمة نوعاً ما، ومن السهل إيجادها. وتستطيع الدخول إلى شبكات 802.11b بتحريك الطيف الراديوي بحوالي 2.4 GHz. وهو جزء مزدحم قليلاً من الطيف الراديوي، والذي تستخدمه أجهزة المايكروويف، الأجهزة الطبية، المصابيح الضوئية المضغوطة، وحتى نوع معين من الهواتف اللاسلكية، وكلها تستطيع أن تحط من أداء الشبكة اللاسلكية عن طريق إشاراتها المتشردة.

بما أن الشبكة اللاسلكية WLAN تعتمد على انتشار الإشارات الراديوية، فإنها تصبح معرضة إلى هجوم لتعطيل الخدمة المزدحم. "مزدحم" هي ما تبدو عليه فقط: الضغط على الموجات الراديوية بمصدر طاقة أقوى لمنع إرسال البيانات. مع أن المهاجمات التقليدية المعتمدة على الحزم كتلك المستخدمة في الشبكات السلكية ممكنة أيضاً، لكن يستطيع الجاسوس باستخدام الشبكة اللاسلكية WLAN مرسل عالي الطاقة 2.4 GHz لمقاطعة الشبكة عن طريق الإرسال على الترددات المعروفة لشبكة 802.11b. الطاقة المشعة الأعظمية للأجهزة اللاسلكية مقصورة أعظمياً على 4 وات، لذلك ليس بالأمر الصعب على أحد ما يتمتع بمعلومات قليلة حول الإلكترونيات

والراديو أن يعدل نقطة الوصول AP لحجب الشبكة المستهدفة. هذا لن يجعل المخرّب معروفاً جداً لدى هيئة الاتصالات الفدرالية FCC، لأنه يقوم باختراق سلسلة من القوانين، لذلك سوف يزيد انتهاك آخر إلى ملفه الحافل.

كيف يمكن استخدام الهجوم لتعطيل الخدمة لأغراض تجسسية؟ قد تعطيك ذريعة للوصول إلى الهدف. لاحظ ما يلي.

تخيل الوضع التالي، تعاني الشبكة من مشاكل مجهولة المصدر كل صباح ولا أحد من الموظفين يعلم ماذا يحصل، وفجأة يظهر رجل مبتسم يرتدي زياً أزرقاً مع بطاقة الهوية المشبوكة على قميصه عند مكتب الاستقبال. "صباح الخير، أنا John Smith من شركة الهاتف. لقد وردنا تقرير بأنكم تعانون من مشاكل في أداء الشبكة، ونظن أن الواقي على أحد خطوط السكة الحديدية يقوم بتوليد تداخل في أمواج الراديو. ومع ذلك يمكنني أن أصلحه. هل يمكنك أن تدلني على مكان الموجهّات لديكم؟" حيث استخدم رجل الإصلاحات المزيف من شركة الهاتف المزيفة جهاز إرسال 2.4 GHz للتشويش على الشبكة اللاسلكية WLAN، لكي يستطيع الدخول إلى المبنى لسرقة المعلومات.

مشاكل مع التكوين الافتراضي

قد تتصور أن مع جميع المساوئ التي تعاني منها الشبكات المحلية اللاسلكية 802.11b WLANs، فإنه لن تسوء الأمور أكثر من ذلك في موضوع الأمن. وأي شخص قد تعرض إلى قضايا الأمن، يعلم أن هناك تناسب عكسي بين سهولة الاستخدام والأمن، ويطبق هذا التناسب أيضاً على المنتجات اللاسلكية. يقوم البائعون بتكوين نقاط الوصول والبطاقات الشبكية لتكون سريعة وسهلة الاستخدام، لكن كل هذا على حساب الأمن.

يصرح أشخاص يسمون أنفسهم بالاسم war drivers (الذين سنعرضهم في المقطع القادم) أن نسبة 50 إلى 80 بالمائة من نقاط الوصول التي يجدونها تتضمن قيم SSID افتراضية وتقنية WEP غير مفعلة. حيث يقوم المستخدمون والمسؤولون بتركيبها بكل بساطة وهي تعمل مباشرة، كما يسعى البائعون إلى هذه البساطة ليبيعوا مزيداً من المنتجات. بعض القضايا التنفيذية التي يمكنك استغلالها ببساطة هي:

- **لا يتم تفعيل تقنية WEP افتراضياً**: الأثر واضح. يستطيع الجاسوس أن يتنصت على الحزم المارة باستخدام برنامج sniffer.
- **مفاتيح افتراضية معروفة لتقنية WEP**: حتى لو كانت تقنية WEP مفعلة، يملك بعض البائعون مفاتيح افتراضية قد لا يغيرها المستخدم الكسول أو الجاهل. هذه المفاتيح معروفة

كثيراً، وإذا تم تحديد نقطة الوصول أو نوع بطاقة واجهة الشبكة من قبل عنوان MAC أو قيمة SSID افتراضية، يستطيع الجاسوس أن يجرب أحد مفاتيح WEP الافتراضية ليتحقق منها.

- **مساوئ الإدارة البعيدة:** تتضمن نقاط الوصول نموذجياً خيارات للإدارة البعيدة والتي تسمح لمدير النظام أن يكوّن إعدادات الشبكة. تتضمن البروتوكولات المستخدمة بروتوكول إدارة الشبكة البسيط SNMP (Simple Network Management Protocol)، بروتوكول Telnet، والبروتوكول HTTP للوصول إلى مستعرض الويب. مشكلة جميع هذه البروتوكولات أنه يتم إرسال بيانات غير مشفرة عبر الشبكة. وأي شخص يتنصت على الشبكة عندما يقوم مدير الشبكة بتسجيل الدخول إلى برنامج الإدارة، يستطيع الوصول إلى كلمة المرور التي تم إدخالها. وإذا لم يكن هذا سيئاً كفاية، في بعض الحالات يمكن ببساطة شديدة الوصول إلى ميزات التكوين المعتمدة على الويب لنقطة الوصول AP. بعد أن ترتبط بالشبكة اللاسلكية، وإذا كنت تعلم عنوان IP لنقطة الوصول (والتي يستطيع برنامج sniffer أن يكشفها)، ما عليك سوى التأشير باستخدام مستعرضك إلى عنوان IP لتنفيذ برنامج مدير التكوين. إن كلمات المرور الافتراضية لنقاط الوصول معروفة جداً، لذلك سوف تملك التحكم الكامل بإعدادات نقطة الوصول إذا لم يتم تغيير كلمة المرور.



لمزيد من المعلومات حول برامج sniffer، ارجع إلى الفصل التاسع.

بالرغم من الاهتمام الكبير الذي تلقته قضايا الأمن اللاسلكي من قبل الشعب والصحافة التجارية خلال الفترة الماضية، إلا أن المستخدمون ومدراء الشبكة يستمرون في استخدام الإعدادت الافتراضية. حيث أن تجاهل الهدف وموقفه بأنه لن يقوم أحد بالتنصت على شبكته، يسّهل حياة الجاسوس كثيراً.

أدوات التنصت على الشبكات اللاسلكية

بعد أن حصلت على معلومات عامة حول نقاط الضعف التي تعاني منها الشبكة اللاسلكية 802.11b، حان الوقت لتفحص بعض الأدوات التي يمكن أن يستخدمها الجاسوس لكشف الشبكة اللاسلكية WLAN. يمكن استخدام تشكيلة واسعة من البرمجيات مع التجهيزات غير المكلفة لاكتشاف واستغلال نقاط الضعف للشبكات اللاسلكية. حيث أتت الكثير من الأدوات والتقنيات للتجسس اللاسلكي من الثقافة الخاصة لشبكة الإنترنت وتسمى "war drivers". من الهام معرفة كيفية تطور البعض من هذه الأدوات والتعرف قليلاً على الأشخاص الذين قاموا بتطويرها.

مقدمة إلى أدوات "war drivers"

يعني المصطلح "war driving"، في المصطلحات الأمنية الحاسبية المشتركة، القيام بتدقيق متحرك للشبكات اللاسلكية. وببساطة أكثر، التجول في السيارة مع حاسب محمول وبطاقة شبكة لاسلكية بحثاً عن شبكات WLANs من أجل التنصت عليها. (الشاحنة التي تملكها والتي تستخدمها للقيام بعمليات المراقبة العرضية مثالية لهذا الأمر. بسخرية، من أجل اختبار أمن شبكة لاسلكية، سوف تستخدم نفس الأساليب تماماً التي يستخدمها الجاسوس لاختراق الشبكة).

أتى المصطلح "war driving" من العملية التخريبية التي كانت تحدث في الثمانينيات وتسمى "war dialing". قبل أن يكون بالإمكان تحديد الحواسب الهدف باستخدام مسح المنافذ، استخدم المخرّبون أجهزة المودم وبرامج مثل THC-Scan أو ToneLoc، لطلب الاتصال من خلال مقاسم الهاتف. يقوم البرنامج بشكل متسلسل الاتصال بعدد من الأرقام ليتحقق من إجابة جهاز مودم آخر. فإذا حصل ذلك فهذا يعني وجود حاسب على الطرف الآخر من رقم الهاتف، سوف يتم تسجيل رقم الهاتف، وسوف يحاول المخرّب اختراق النظام في وقت لاحق.

في خريف عام 2000، أخذ المستشار الأمني الحاسبي في كاليفورنيا Pete Shipley حاسباً محمولاً مجهزاً ببطاقة شبكة لاسلكية، برنامجاً أساسياً لاكتشاف الشبكات اللاسلكية WLAN، وجهاز القمر الصناعي لتحديد الموقع الشامل GPS (Global Positioning Satellite)، وبدأ يجول الشوارع في منطقة Bay. بعد مرور 18 شهراً، اكتشف Shipley أكثر من 9000 نقطة وصول AP. وحوالي 95 بالمائة من هذه الشبكات لم تكن تستخدم تقنية WEP وكان من السهل جداً اختراقها. نشر Shipley هذه الدراسة ولقّب هذا التدقيق للشبكات اللاسلكية باسم "war driving". وقد علق هذا المصطلح في آذان وسائل الإعلام بالإضافة إلى مجتمعات الأمن والحواسب.

في عام 2001، تطورت نسبة سكانية كبيرة لعمل "war drivers" نتيجة إصدار أداة كشف الشبكات اللاسلكية WLAN في نظام التشغيل Windows وتسمى NetStumbler وكمية كبيرة من المعلومات المشاركة عبر شبكة الإنترنت. باستخدام هذه الأداة ما عليك سوى تركيب بطاقة شبكة لاسلكية في حاسبك المحمول، تنفيذ البرنامج، وقيادة السيارة. عندما تجد الأداة الشبكة فإنها تعرض قيمة SSID، وفيما إذا كانت تقنية WEP مفعّلة، ومعلومات أخرى حول الشبكة. وإذا كان لديك جهاز GPS موصول بحاسبك، سيقوم برنامج NetStumbler بتحديد موقع الشبكة.

بما أن برنامج NetStumbler سهل الاستخدام، أصبحت عملية "war driving" شائعة في جميع أنحاء العالم. تجمع قواعد البيانات المعلومات حول الشبكات التي تم اكتشافها، نُشرت خرائط حول مواقع نقاط الوصول، وتوجد مناقشات شعبية فعالة حول أفضل التجهيزات والبرمجيات التي يمكن استخدامها لاكتشاف الشبكات اللاسلكية WLAN.

هناك جانبان لعملية "war driving". الجانب المضيء والسعيد هو أن الكثير من الأشخاص يقودون سياراتهم بحثاً عن الشبكات اللاسلكية كنشاط غير مؤذ أبداً، حيث لا يحاول هؤلاء اختراق الشبكات التي يعثرون عليها، فهم يقومون بتحديد الشبكات فقط. ويعتبرون هذا الأمر مثل هواية عبر خطوط التقنية المتطورة، صيد الكتروني، مع التفاخر بعدد الشبكات التي يجدونها. وهناك أيضاً الجانب المظلم من الموضوع. بعد أن يتم العثور على شبكة WLAN وخاصة تلك التي تكون فيها تقنية WEP غير مفعّلة، وهنا يتحول الأمر إلى ارتكاب أفعال خارجة عن القانون، حيث مجرد اختراق الشبكة يعد جريمة حاسبية.

ما هي العلاقة بين كل هذه الخلفية التاريخية والتجسس؟ الأمر بسيط، لقد مهدت عملية "war driving" الطريق لك لتكون جاسوساً لاسلكياً مبتدئاً. حيث تتوفر الأدوات، التقنيات، مجموعات دعم غير رسمية لتسهّل عليك ولأي شخص آخر مهتم بالتنصت على الشبكات اللاسلكية WLAN.

أساليب: الشبكات اللاسلكية، أنت على مرأى مني

لا يقتصر استخدام الشبكات اللاسلكية 802.11b على استعراض الويب أو الوصول العام للشبكة، إنما أصبحت الشبكات اللاسلكية 802.11b شائعة الاستخدام في كاميرات المراقبة اللاسلكية، ويمكن أن يستغل الجواسيس نقاط الضعف نفسها بطرق جديدة.

في شهر آب (أغسطس) عام 2002، ظهر تقرير حول وكالة أنظمة المعلومات لوزارة الدفاع DISA (Department of Defense Information Systems Agency). الوكالة Arlington التي مقرها في ولاية Virginia مسؤولة عن أمن شبكات وأنظمة الأوامر والتحكم لوزارة الدفاع الأمريكية. اكتشف مستشار كان يستخدم برنامج NetStumbler كاميرات مراقبة عند مسؤولي الوكالة والتي كانت جزءاً من شبكة 802.11b. لم تكن تقنية WEP مفعّلة وأظهر البرنامج قيمة AP SSID تحت اسم "AP-BLDG12،" والتي منحت موقعها الفيزيائي لأنها أرجعت إلى مكان معلّم بوضوح من الخارج بالاسم BLDG 12. لو كان جاسوساً لاستطاع بسهولة التنصت على إرسال الفيديو (مع العلم من أين تم توليدها نتيجة لاسم SSID) ومع قليل من الجهد لكان استطاع أن يتحكم بالنظام أو حتى حشر صور مزيفة للحراس على الشاشات. وهذا أمر مقلق جداً إذا أخذنا بعين الاعتبار الوكالة المقصودة.

حتى الألعاب يمكن استخدامها كجواسيس. حيث تقدّم لعبة AIBO، وهي كلب آلي ذو مزايا متطورة من شركة Sony، خيار 802.11b والذي يمكن أن تستخدمه للتحكم بالكلب عن بعد من حاسب محمول أو حاسب مكتبي باستخدام برنامج المستكشف AIBO، يرسل الكلب الآلي الصور والأصوات إلى الحاسب الذي يتحكم به. خيارات التنصت لا نهاية لها، لأنه يمكن سرقة

اللعبة ومن ثم تحريكها في غرفة خالية بحثاً عن معلومات مشوقة. فإذا كنت تستخدم برنامج NetStumbler ووجدت قيمة SSID باسم AIBONET، يوجد هناك كلب لاسلكي في الطرف الآخر. وقيمة WEP الافتراضية له هي AIBO2.

منتج آخر مناسب جداً للتجسس هو الكاميرا اللاسلكية X-10. يبدو لك لبرهة أن الوظائف الإضافية للكاميرا كانت تظهر في كل موقع ويب كنت تزوره، وتبدو مثل كاميرا فيديو صغيرة حجمها يساوي حجم كرة الغولف. تبث الكاميرا بتردد 2.4 GHz إلى مستقبل لاسلكي بعيد، والذي يعرض الصور بعدئذ على التلفاز، الفيديو، أو الحاسب الشخصي. مداها يصل إلى 30 قدماً. ويوجد أمر صغير تهمل X-10 ذكره وهو أنه لا توجد أية ميزات أمنية لتمنع شخصاً آخر يملك جهاز مستقبل X-10 من التنصت على إرسالات الفيديو. حيث أصبح المتطفلون يقودون سياراتهم ويستعرضون الفيديو من غرف النوم، أسرّة الأطفال، وأنظمة الحماية المنزلية. توجد كاميرات أخرى في الأسواق وتبث بتردد 900 MHz ويمكن أن يتم التجسس عليها باستخدام ماسحات راديو متطورة. حيث تتلقى ماسحة Icom R-3 الإرسالات الصوتية، وتعرض أيضاً إرسالات الفيديو اللاسلكية. بالرغم من أنها تعمل على البطاريات ولها مدى محدود، إلا أنه يمكن استخدامها للتنصت على أنظمة المراقبة اللاسلكية.

مضبوط: إضراب الإمبراطورية

في الحقيقة لم توجد نشاطات شرعية وإجرامية ضد المتطفلين لاسلكياً حتى شهر تموز (يوليو) من عام 2002، عندما تم اتهام Stefan Puffer فدرالياً من قبل هيئة محلفين بتهمة الخداع. Puffer مستشار أمني حاسبي يبلغ من العمر 33 عاماً في Houston، ولاية Texas. حيث عرض في الثامن عشر من شهر آذار (مارس) عام 2002، إلى رئيس قسم Harris County IT ومراسل صحفي من جريدة Houston Chronicle أن الشبكة اللاسلكية WLAN لمساعده كانت غير مؤمنة. كان يقود السيارة منذ حوالي شهر وعثر على شبكة County، وقرر أن يكون مواطناً صالحاً (أنجز Puffer بعض الأعمال الحاسبية لصالح County في وقت سابق).

صرح County أنه تم إجبارهم على إطفاء الشبكة اللاسلكية، مما تسبب في خسائر تصل إلى قيمة 5,000 دولار أمريكي (وهو المبلغ النموذجي للتدخل الفدرالي)، وقام مكتب التحقيقات الفدرالي بإجراء التحقيقات. والمثير في الموضوع أن County صرح أنه لم يتم كشف أية ملفات ولم يعط الموظفون سبباً عن إطفاء الشبكة بدلاً من تأمينها. وفي شهر أيلول (سبتمبر) عام 2002، أوقف County تحقيقه الخاص ضد Puffer وقال أنه لن يصدر تقريراً نهائياً أو تهم صحفية.

وفي شهر شباط (فبراير) عام 2003، قررت هيئة المحلفين بعد 15 دقيقة من المناقشة، أن Puffer لم يقم بالتخطيط لإلحاق أي أذى لنظام County، وتمت تبرئته. في حال تمت إدانة Puffer كان سيواجه عقوبة بالسجن قد تصل إلى خمس سنوات وغرامة بقيمة 250,000 دولار أمريكي لكل تهمة.

من الواضح أن هذه القضية هي رسالة تحذيرية من وزارة العدل إلى "war drivers" وأن الأمر جدي حول المقاضاة الفعالة. وفعلياً استفاد المخرّبون والجواسيس الذين يقتحمون الشبكات اللاسلكية.

التجهيزات

على خلاف الأشكال الأخرى من التجسس ذو التقنية المتطورة، لا تحتاج عملية اكتشاف شبكة لاسلكية WLAN والتنصت عليها لتجهيزات معقدة أو مكلفة. في الواقع، ربما قد تملك مكونات التجهيزات الأساسية ويمكنك شراء التجهيزات المتبقية مقابل بضع مئات من الدولارات.

الحواسب المحمولة LAPTOPS: مع أنه يمكنك أن تتنصت على شبكة لاسلكية باستخدام حاسب مكتبي، إلا أن الحواسب المحمولة ملائمة أكثر لهذه المهمة. ضع حاسباً محمولاً مجهّزاً بشكل مناسب على مقعد سيارتك، خبأه على أرضية السيارة، أو أخفه ضمن حقيبة للظهر، والآن أصبحت مستعداً للانطلاق.

حتى أنك لا تحتاج إلى حاسب محمول حديث جداً، حيث يعمل النموذج الأقدم بذاكرة كافية ومعالج يستطيع تنفيذ نظام التشغيل Windows 98 أو Linux، بصورة ممتازة تماماً مثل حاسب محمول بمعالج Pentium IV. يحتاج الحاسب المحمول مقبس بطاقة PC فارغ بالإضافة إلى منفذ تسلسلي في حال أردت وصل جهاز GPS لتسجيل مواقع الشبكة.

الأمر الذي تريد أخذه بعين الاعتبار هو قراءة الشاشة. حيث قد تصعّب أشعة الشمس الساطعة رؤية محتويات الشاشة، لذا قد ترغب بحاسب محمول يعمل جيداً خارج المنزل. يمكنك تعويض مدى قراءة الشاشة بتغيير خيارات الألوان في نظام التشغيل، مثلاً استخدام نظام ألوان أبيض وأسود أحادي اللون.

بالطبع يمكن أن تستخدم أي حاسب محمول، لكن يفضل استخدام الحواسب الأصغر حجماً والأخف وزناً. وهي متعددة الاستعمالات أكثر لأنه يمكن استخدامها في السيارة كما يمكن إخفاءها في حقيبة ظهر، وعندما تريد المراقبة قم بتشغيل الحاسب المحمول ونفّذ برنامج المسح عندما تتجول.

تحد بطاريات الحاسب المحمول نشاطات الجاسوس إلى ما بين ساعتين وأربع ساعات، لذلك إذا قررت إنجاز مراقبة إضافية، اجلب معك بطاريات بديلة أو استخدم مصدر طاقة خارجي في سيارتك.

حواسب الجيب POCKET PCS: للحصول على تجسس لاسلكي خفي تماماً، يمكنك استخدام حاسب جيب Pocket PC. ومن أفضل الأنواع iPAQs من شركة Compaq بسبب صغر حجمها، توافقيتها مع بطاقات الشبكة اللاسلكية ووحدات GPS، وقدرتها على تشغيل أدوات الاكتشاف الشائعة لنظامي Windows وLinux.

جهاز iPAQ مثالي لتحديد موقع الشبكات اللاسلكية WLAN بشكل سري داخل المباني وخارجها، وتسمى عملية المسح على الأقدام "war walking". كما توجد برامج sniffer متوفرة لحواسب الجيب وبالتالي يمكنك التنصت على الحزم بعد أن تعثر على الشبكة.



لمزيد من المعلومات حول المصطلحات الخاصة بأمن الحواسب والتنصت الحاسبي، اتبع الرابط www.warchalking.org.

بطاقات الشبكة NETWORKING CARDS: قبل أن تبدأ بالتنصت على شبكة لاسلكية WLAN تحتاج إلى بطاقة واجهة شبكة لاسلكية لحاسبك المحمول. تدخل بطاقات الشبكة اللاسلكية إلى داخل مقبس بطاقة PC مع بروز الهوائي بطول أنش تقريباً من خارج المقبس (توجد بعض النماذج مثل 3Com Office Connect ذات هوائي قابل للسحب). كما انخفضت أسعار بطاقات واجهة الشبكة اللاسلكية بصورة مذهلة، بعد انتشار شعبية شبكات 802.11b، وتبلغ قيمة بطاقة شبكة متطورة إلى أقل من 100 دولار أمريكي.

تأتي النماذج الأحدث من الحواسب المحمولة مجهزة ببطاقات شبكة لاسلكية مدمجة. حيث بدلاً من أن يكون هوائي البطاقة ظاهراً من المقبس مثل البطاقات الإضافية، يتم تركيب الهوائي داخلياً ضمن صندوق الحاسب المحمول. فإذا كنت جالساً على مقعد في الحديقة على طرف الشارع المقابل من المكتب المستهدف، فمن الصعب معرفة إذا كان حاسبك المحمول يدعم بطاقة لاسلكية.

توجد ثلاث رقاقات تدعم أجهزة 802.11b: Hermes، Prism-2، و Aironet.

- Hermes. تأتي منتجات Hermes تحت اسم Lucent، Wavelan، ORiNOCO، Avaya، RoamAbout، و BuffaloTechnology. يتمتع هذا النوع باستقبال أفضل من بطاقات Prism وتقدّم وصلة لهوائي خارجي.
- Prism. يتم تصنيعها من قبل شركات SMC، D-Link، Linksys، Microsoft وغيرها. وهي الرقاقات الأكثر شيوعاً في الأسواق، تتميز بأنها غير مكلفة، ولها مدى أقصر من بطاقات Hermes. ميزتها الأساسية هي إمكانية وضعها ضمن نمط مشوش للتنصت على حزم 802.11b خام، وقد طُورت أدوات برمجية كثيرة لدعم هذا النوع من البطاقات.
- Aironet. وهي أفضل أنواع بطاقات الشبكة اللاسلكية ذات أداء عال، مصنّعة من قبل شركة Cisco. وهي ليست شائعة مثل سابقاتها ولا تملك الكثير من الأدوات التي تدعمها.

تملك كل من هذه الرقاقات مطورها الخاص، بحيث لا تعمل الأداة البرمجية المطورة لبطاقات Hermes على بطاقات Prism. ومثال تقليدي للأداة الشائعة NetStumbler، والمصممة لتعمل

مع بطاقات Hermes فقط، ومع ذلك توجد نسخة جديدة من البرنامج تعمل مع بطاقات Prism إذا كنت تستخدم Windows XP.

بما أن البطاقات اللاسلكية غير مكلفة، فمن الأفضل أن تشتري كلا النوعين Prism وHermes لتستفيد من الأدوات البرمجية الكثيرة المتوفرة. حالياً لا توجد أداة تنصت لاسلكية محددة لرقاقة محددة، وسوف ترغب باستخدام برمجيات متعددة بناءً على الحاجة. ينصح حالياً باستخدام البطاقتين ORiNOCO Gold (Hermes) وProxim RangeLAN-DS (Prism 2).

أساليب: "war chalking"

لقد منح استخدام حاسب الجيب Pocket PC المخفي أو حاسب محمول صغير من أجل عملية المسح على الأقدام أو "war walking"، فكرة جديدة تسمى "war chalking". حيث اخترع المتشردون، خلال كساد النشاط الوظيفي، سلسلة من الرموز لجعل المسافرين مطّلعين على الأوضاع المحلية. مثلاً، قد تعني إشارة معينة على الجدار أن هناك شخص لطيف مستعد أن يشاركك بطعامه، أو إشارة تحذير عن وجود كلب شرس. وفي صيف عام 2002، قام مصمم الإنترنت Matt Jones بتحقيق فكرته المذهلة وهي ما سماه "war chalking". حيث نشر Jones سلسلة من الرموز الموحدة مرتبطة بالشبكات اللاسلكية والتي يمكن أن ترسم على الأبنية أو أرصفة المشاة عندما يتم اكتشاف شبكة لاسلكية WLAN (انظر الشكل 1-11). فإذا رأى أحد المارة الذي يملك حاسباً محمولاً وبطاقة شبكة لاسلكية رمزاً معيناً خارج بناء ما، سوف يعلم أنه بإمكانه استخدام اتصال مجاني بالإنترنت من مكان قريب. اعتبر بعض المستشارون الأمنيون هذه الرموز نموذج سخرية لا أكثر ولا أقل. لكن من جهة ثانية، اعتقد مكتب التحقيقات الفدرالي أنه عمل جدي وخطير أن يكون على مرأى الجميع رموز غريبة مخططة خارج الأبنية.

KEY	SYMBOL
Open Node	SSID)(Bandwidth
Closed Node	SSID O
WEP Node	SSID Access contact (W) Bandwidth

الشكل (1-11) رموز "war chalking". تظهر قيم SSID وعرض الحزمة للشبكة المحلية التي تم اكتشافها إلى جانب الرمز. تتضمن منطقة الوصول للاتصال معلومات اتصال معروفة، مثل رقم الهاتف أو البريد الإلكتروني، للوصول إلى الشبكة اللاسلكية المحمية بتقنية WEP.

ويما أنك جاسوس ذكي، فلن تقوم أبداً برسم هذه الرموز على بناء هدفك لكي لا تكشفه للآخرين، والآن بما أنك تعرف هذه الرموز فقد تسهل مهمتك كثيراً عندما تراها في طريقك.

الهوائيات ANTENNAS: تحوي جميع بطاقات الشبكة اللاسلكية هوائيات صغيرة، مركبة داخلياً، والمصممة لتحوي مجالاً مناسباً للشبكات المنزلية والمكتبية. لكن الاعتماد على مجال الهوائي النظامي يحصرك في اكتشاف وكشف الشبكات اللاسلكية WLAN. أما إذا كنت تستخدم هوائي خارجي، فسوف تكون قادراً على إيجاد شبكات أكثر والبقاء بعيداً عن الهدف لكي لا يتم كشفك.

أما بالنسبة للمراقبة المتحركة، فمن المهم أن تختار بطاقة شبكة لاسلكية تدعم هوائي خارجي. من الصعب العثور على هذا النوع بسهولة، ومع أنه توجد مخططات لتعديل البطاقات لكي تقبل هوائيات خارجية، إلا أنه من الأسهل شراء بطاقة خارجية. تحوي الأنواع ORiNOCO Gold و Proxim RangeLAN-DS مقابس لتتصل بهوائي خارجي. كما تحوي معظم الهوائيات التجارية سلك ينتهي بوصلة من النوع N (وهي وصلة معدنية كبيرة تستخدم نموذجياً مع منتجات الراديو التجارية وغير المحترفة). تحتاج إلى سلك محول إضافي لتصل البطاقة إلى سلك الهوائي، لكن المحولات الإضافية سهلة الكسر، لذلك من المهم عدم ضربها أو ثنيها.

استخدم "war drivers" بالأصل هوائيات صغيرة مصممة خصيصاً لتمديد مجال الشبكات WLAN. ومع زيادة شعبية "war driving"، أصبح هناك خيارات أكثر سرية يمكن استخدامها.

يجب أن تُصمم الهوائيات لتعمل على الترددات 2.4 GHz، وقد لا تعمل الهوائيات الأقدم. مثلاً، إن محاولة استخدام هوائي التلفاز للتنصت اللاسلكي قد لا يكون فعالاً، لأنه تم تصميم أفضل أداء لهوائي التلفاز أن يستقبل إشارات ضمن المجال الترددي 50 إلى 220 MHz.

عندما تطلع على مواصفات الهوائي، سوف ترى رقماً متبوعاً بكلمة "dBi"، والتي تشير إلى ربح الهوائي — أي كمية الإشارة التي يستطيع الهوائي أن يلتقطها مقارنة مع هوائي آخر. كلما زاد رقم الربح، كلما استطاع الهوائي استقبال الإشارات الضعيفة بشكل أفضل. رقم الربح للهوائيات الصغيرة حوالي 5 dBi، أما للهوائيات الأكبر فهو أكثر من 10 dBi.

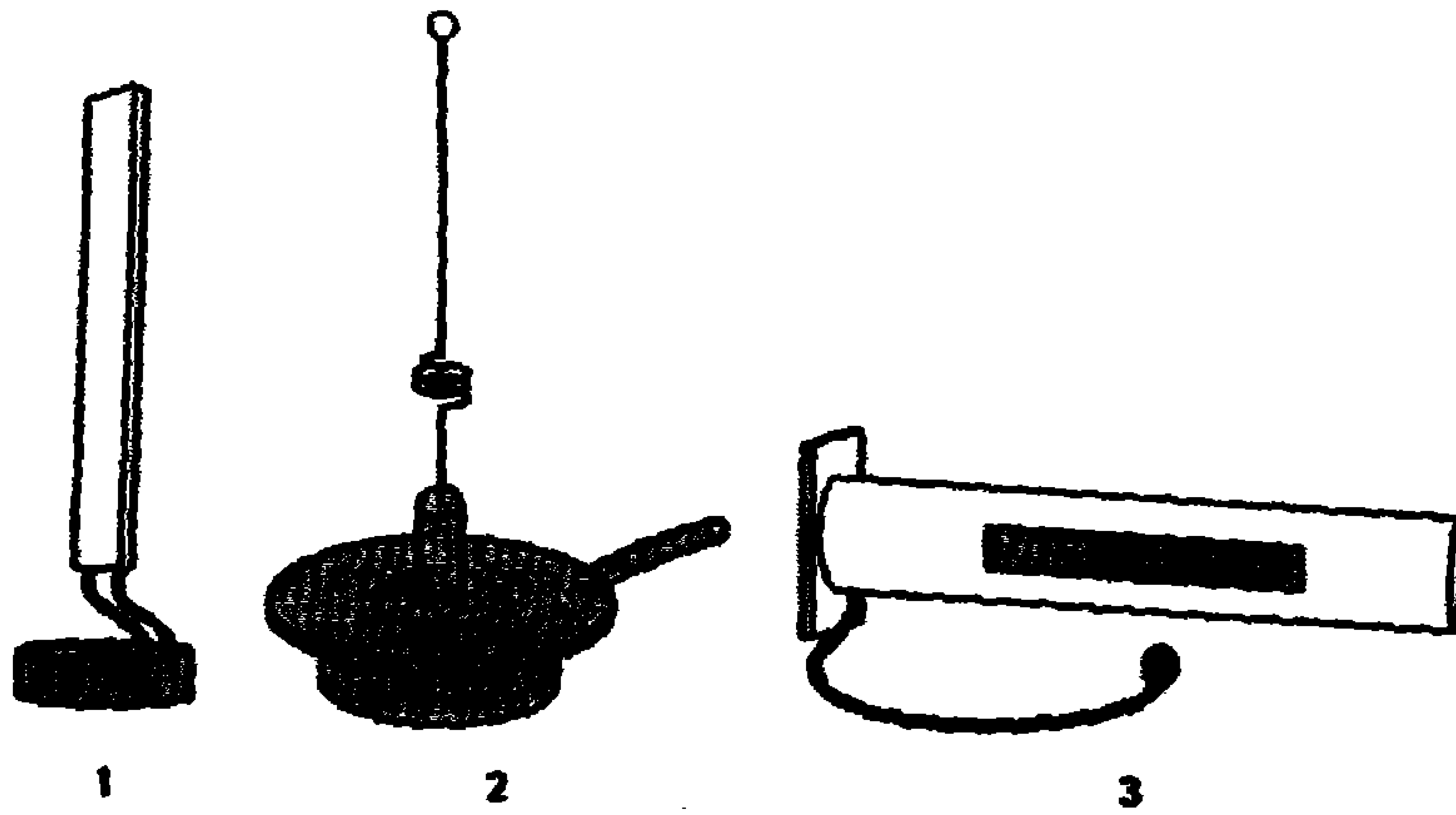
لا تعمل جميع أنواع الهوائيات المصممة لترسل وتستقبل بمدى ترددي 2.4 GHz بشكل متماثل. يوجد بشكل عام نوعان للهوائيات، اتجاهي كلي واتجاهي، وكل منها ذات أهداف مختلفة (انظر الشكل 2-11).

- **الهوائيات كلية الاتجاه Omni-directional antennas**: يرسل ويستقبل هذا النوع من الهوائيات الإشارات الراديوية في جميع الاتجاهات. وهذا النوع مثالي لاكتشاف الشبكات اللاسلكية.

توجد بعض النماذج ذات قواعد مغناطيسية للتركيب الخفي على سطوح السيارات. تبلغ كلفة الهوائيات كلية الاتجاه والمناسبة للتجسس اللاسلكي بين 50 و 100 دولار أمريكي.

- **الهوائيات الموجهة Directional antennas**: تم تصميم هذا النوع من الهوائيات لتركز قوة الإشارة على الاتجاه الذي تشير إليه وتقلص قوة الإشارات القادمة من الاتجاهات الأخرى. تعد هذه الهوائيات مثالية لتستهدف شبكة لاسلكية معروفة. يمكنك توجيهها إلى بناء لتلتقط الإشارة عن بعد أو إذا كنت قريباً. وتستقبل إشارات أضعف من أعماق المبنى والتي قد لا يستطيع الهوائي كلي الاتجاه التقاطها. الهوائيات الموجهة أكبر حجماً من الهوائيات كلية الاتجاه. يمكنك أن تستخدمها بنفسك في السيارة، لكن إذا كنت توجه الهوائي من مكان ثابت عن بعد، استخدم مرجل ثلاثي القوام الذي يستخدم للكاميرا أو شيء آخر لتقوم بتثبيتها.

تبلغ كلفة الهوائيات الموجهة والمناسبة للتجسس اللاسلكي أقل من 200 دولار أمريكي.



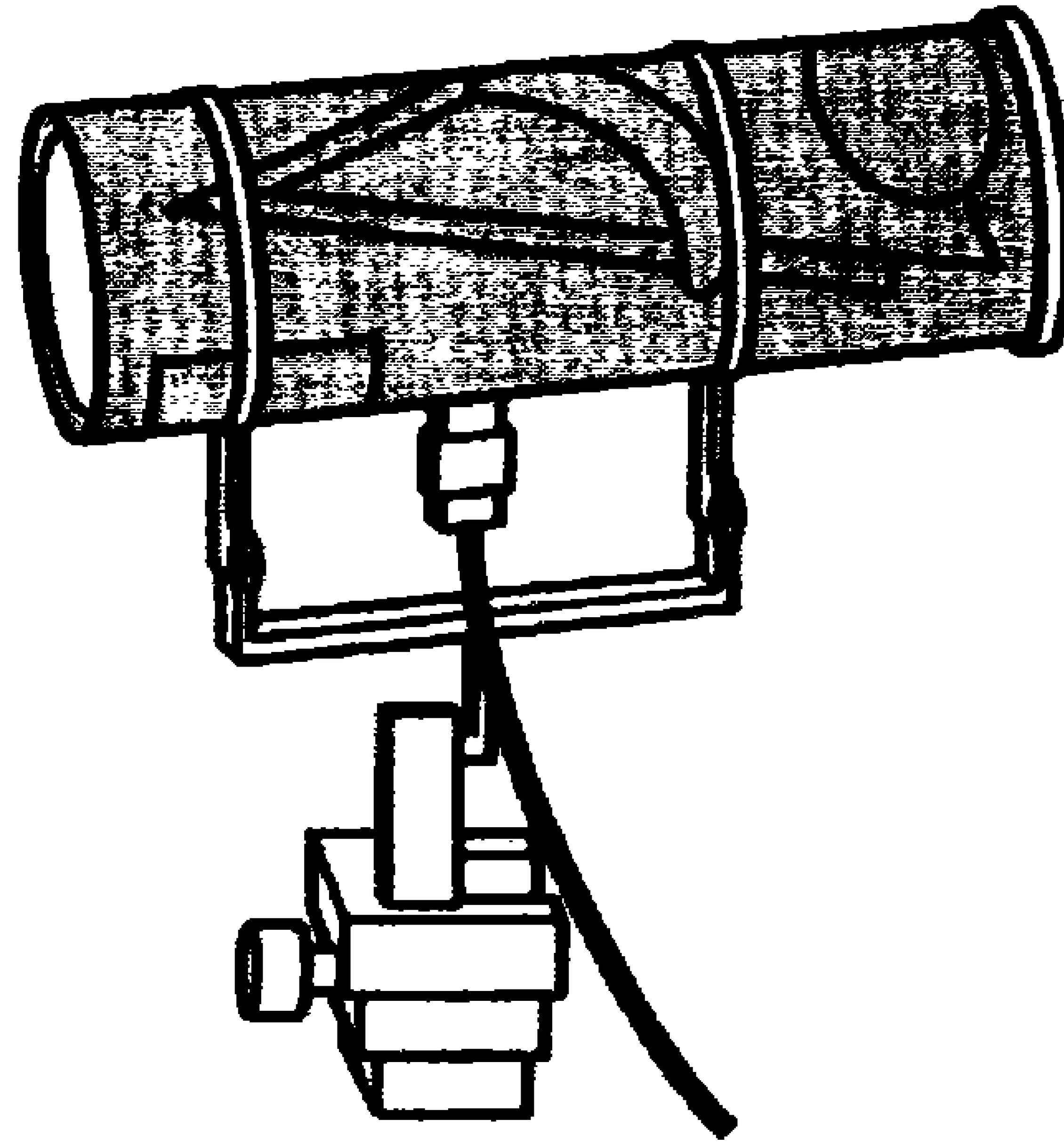
الشكل (2-11) ثلاثة هوائيات ذات تردد 2.4 GHz من اليسار إلى اليمين:
1- Lucent Range Extender، وهي مناسبة للاستخدامات الأقدم.
2- magnetic mount، هوائي كلي الاتجاه يستخدم غالباً للتنصت في السيارة. 3- هوائي موجه مغلف Yagi جيد للبحث عن الشبكات اللاسلكية على مسافة ليست قريبة.

إذا كانت لديك ميزانية، هناك عدد من الموارد التعليمية على الإنترنت من أجل تصميم هوائيات موجهة ذات مدى ترددي 2.4 GHz باستخدام مواد يومية، موجودة في المطبخ، مثل القهوة،

الشطة، والعلب المعدنية لرقائق Pringles (تنظر الشكل 3-11). في الواقع تستطيع هذه المواد بكلفة 5 دولارات متفرقة، دون أن نحسب محتويات العلبة المعدنية، أن تنتج لنا هوائي تجاري. هذا النوع من الهوائيات مثالي للجاسوس الواعي والذي يؤمن في ضرورة إعادة الاستخدام.



يمكن أن تجد مراجعة ممتازة حول الهوائيات المنزلية على الرابط .www.turnpoint.net/wireless/has.gtml

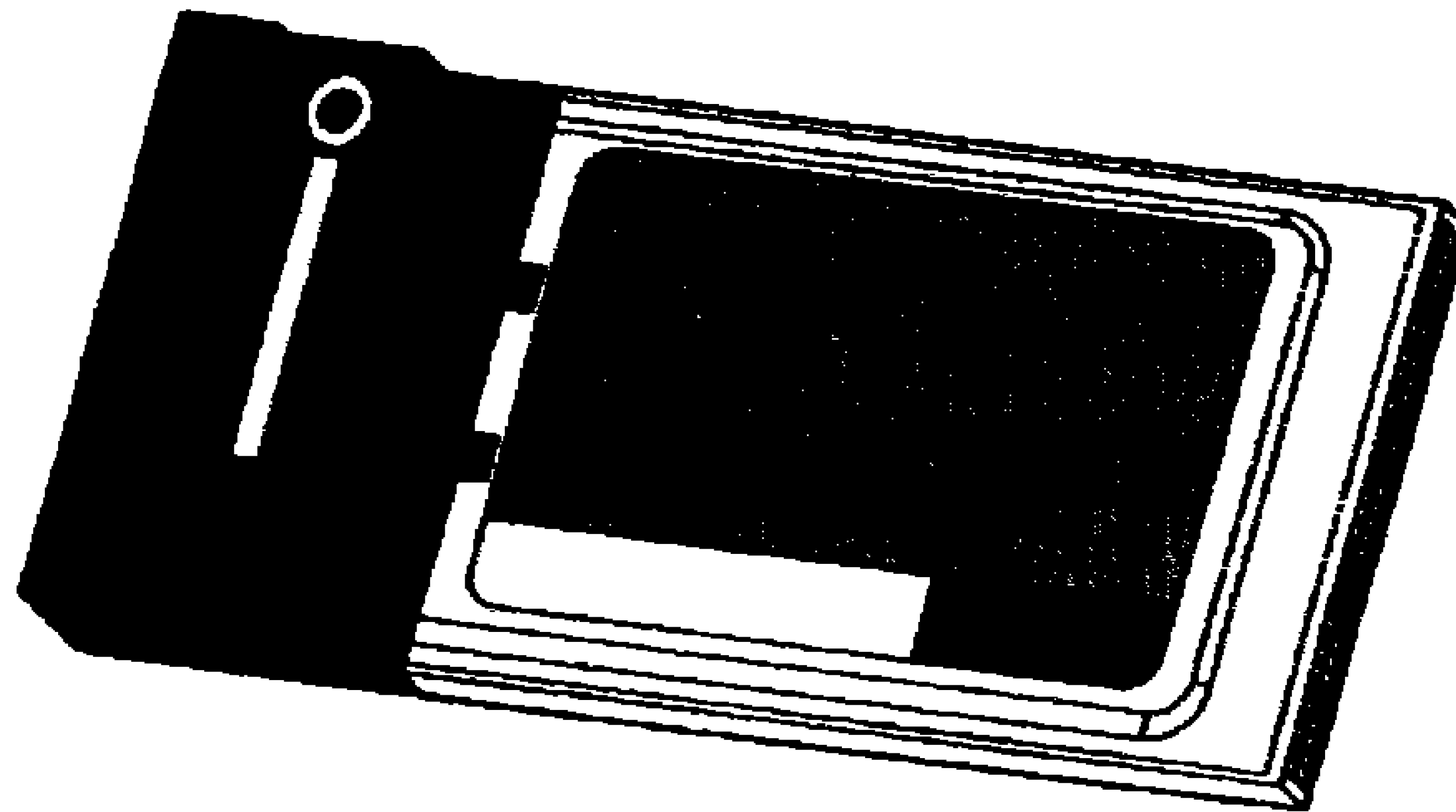


الشكل (3-11) هوائي خفي: هوائي موجه مصنوع من علبة معدنية لرقائق Pringles.

لا تحتاج صناعة الهوائيات المنزلية إلى معلومات تقنية كبيرة، ويمكن إعدادها بسرعة وسهولة نسبية. بينما تتطلب الهوائيات كلية الاتجاه معلومات وعمل أكثر. وما لم تملك راديو أو خلفية إلكترونية، فمن الأفضل لك أن تشتري هوائي تجاري كلي الاتجاه.

وسائل التجارة: البحث عن الذهب

إذا بدأت تطلع على مواقع الويب الخاصة بـ"war drivers"، وقرأت بعض النقاشات في المنتديات، بالتأكيد سوف تسمع عن ORiNOCO Gold Card (البطاقة الذهبية) (انظر الشكل 4-11). حيث أن هذه البطاقة تتلقى علامات أداء مرتفعة جداً، وتم تصنيعها من قبل ORiNOCO Wireless، والتي اكتسبتها شركة Proxim في شهر آب عام 2002، وقامت بتصميمها شركة Lucent. كما أنه تملك أيضاً مقبساً صغيراً لهوائي خارجي والذي يمكن أن يزيد المجال بشكل كبير جداً.



الشكل (11-4) البطاقة اللاسلكية الذهبية لشركة ORiNOCO. غطاء الهوائي على يسار البطاقة.

يأتي برنامج يسمى Client Manager مع بطاقة واجهة الشبكة، ويدعم مسح الشبكات اللاسلكية WLAN مباشرة، ولكي تمسح الشبكات اللاسلكية WLAN اتبع الخطوات التالية:

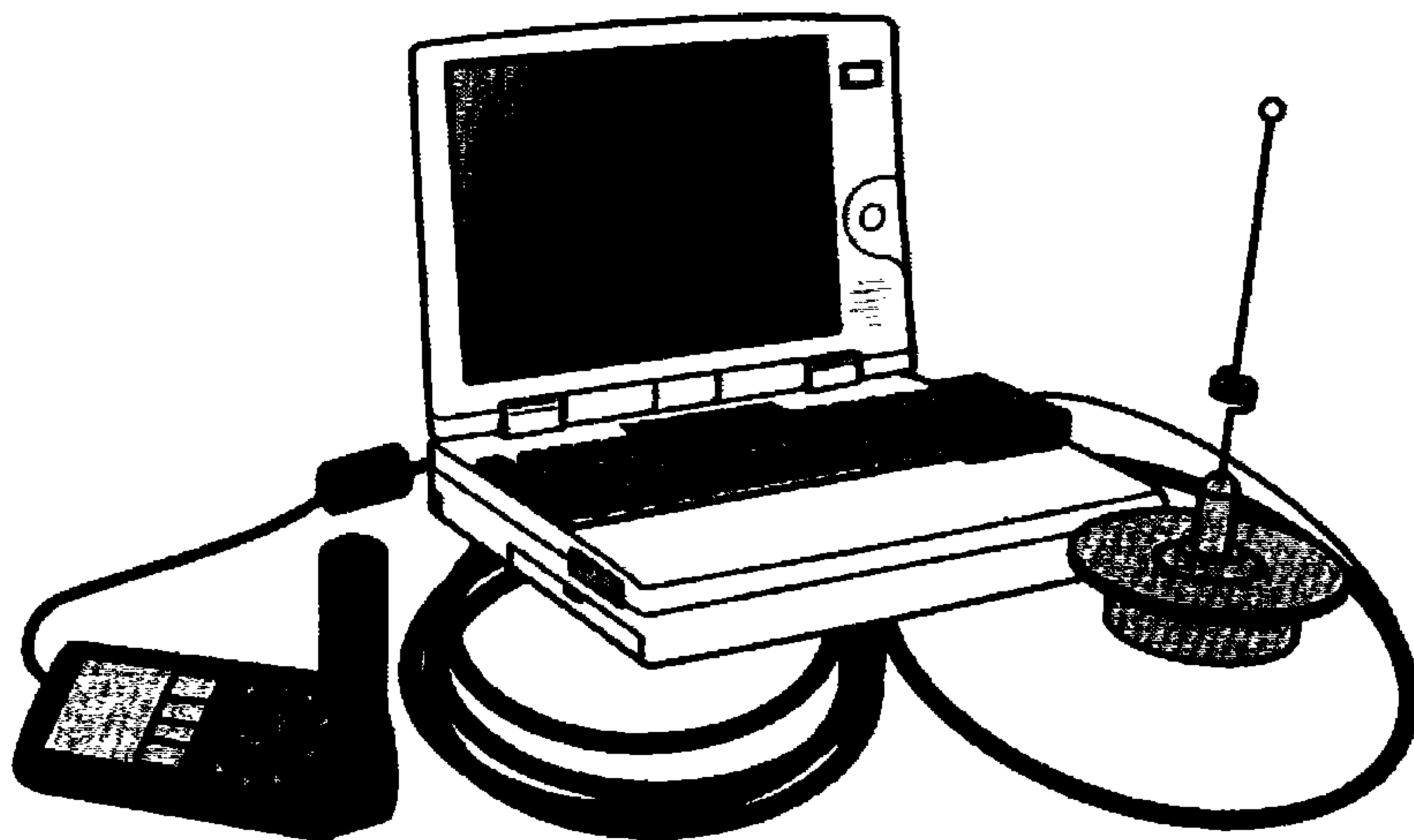
1. نفّذ التطبيق Client Manager.
2. من قائمة Actions، اختر الأمر Add/Edit Configuration Profile.
3. قم بإنشاء تشكيل جانبي (profile) مع منح SSID القيمة "Any" أو null. يوجّه هذا الأمر بطاقة واجهة الشبكة لتبحث عن الشبكات اللاسلكية القريبة.
4. قم بتعيين التشكيل الجانبي الجديد، بالتشكيل الجانبي للتكوين الحالي.
5. من قائمة Advanced، اختر الأمر Site Monitor.

مع أن التطبيق Client Manager لا يزودك بكثير من المعلومات حول الشبكة اللاسلكية WLAN كما تفعل الأداة NetStumbler أو الأدوات الأخرى، إلا أنه مع ذلك برنامج استطلاع خدمي جيد.

تركيب الهوائي: والآن بعد أن حصلت على هوائي، أين يجب أن تركّبه؟ إذا كنت في مركبة، فقد ترغب بحد الغطاء من جسم السيارة وأي تداخل كهرطيسي. كما ترغب بأن لا يكون الهوائي مكشوفاً جداً، وأن لا تركبه بصورة دائمة فقط في حالة اضطررت لإزالة الدليل بسرعة. نموذجياً يقوم "war drivers" باستخدام هوائي مركب مغناطيسياً ويمررون الكبل المحوري خارج نافذة مفتوحة أو من غطاء السيارة المفتوح. ويمكن أيضاً التوجيه عبر خلفية السيارة وخارج صندوق السيارة، وهذا أفضل لأن الكبل لن يتعرض إلى الضرر كثيراً. لكن عليك أن تحذر من

ألا تقرض كبل الهوائي، عن طريق إغلاق الباب فوقه أو رفع النافذة إليه. فإذا تضرر الكبل يمكن أن يقلص قوة الإشارة، وأحياناً يسوء الأمر كثيراً وكأنك لا تملك هوائي أصلاً.

وحدات تحديد الموقع الشامل GPS. ترتبط أدوات اكتشاف الشبكات اللاسلكية WLAN مثل NetStumbler وغيرها مع وحدات تحديد الموقع الشامل GPS (Global Positioning Satellite). وحد ة GPS هي عبارة عن جهاز إلكتروني صغير أصغر بقليل من جهاز التحكم بالتلفاز، ويعرض خط العرض وخط الطول الحالي لموقعك، ويستخدم بروتوكول معتمد على معيار ASCII ويسمى NMEA 0183 لنقل المعلومات إلى حاسب أو جهاز آخر (انظر الشكل 5-11). لقد كان البحارون المستخدمين الأصليين لوحدات GPS على نطاق واسع، وطورت الجمعية الوطنية للإلكترونيات البحرية معياراً للعمل مع الملاح الآلي وتجهيزات الإبحار الأخرى.



الشكل (11-5) حاسب محمول من طراز Toshiba Libretto موصول بالجهازين Garmin III + GPS وجاهز للاستكشاف اللاسلكي.

يوصل كبل تجاري، والذي يختلف بحسب المصنّع، وحدة GPS إلى المنفذ التسلسلي للحاسب المحمول. لكن منفذ USB يستبدل ببطئ الأجهزة التسلسلية ولا تحتوي بعض الحواسب المحمولة الجديدة منافذ تسلسلية. وبدأ مصنّعو وحدات GPS الاتجاه نحو واجهات USB، حيث إذا لم يكن لديك منفذ تسلسلي يجب أن تستخدم محول USB إلى المنفذ التسلسلي (USB-to-serial adaptor).

إذا تضمن الحاسب المحمول وحدة GPS متصلة به، وكانت الأداة NetStumbler أو غيرها تعمل، يتم تسجيل الموقع الجغرافي للشبكة عندما يتم اكتشافها. ومن ثم يمكن نقل هذه

المعلومات إلى برامج التحويل الإلكتروني للإظهار مرئياً جميع الشبكات اللاسلكية التي تم اكتشافها. يتم عرض الشبكات اللاسلكية باستخدام أيقونات مختلفة تشير إذا كانت تقنية WEP مفعّلة أم لا. هذا الأمر يسهّل كثيراً مهمتك في التعرّف على الأهداف المحتملة.

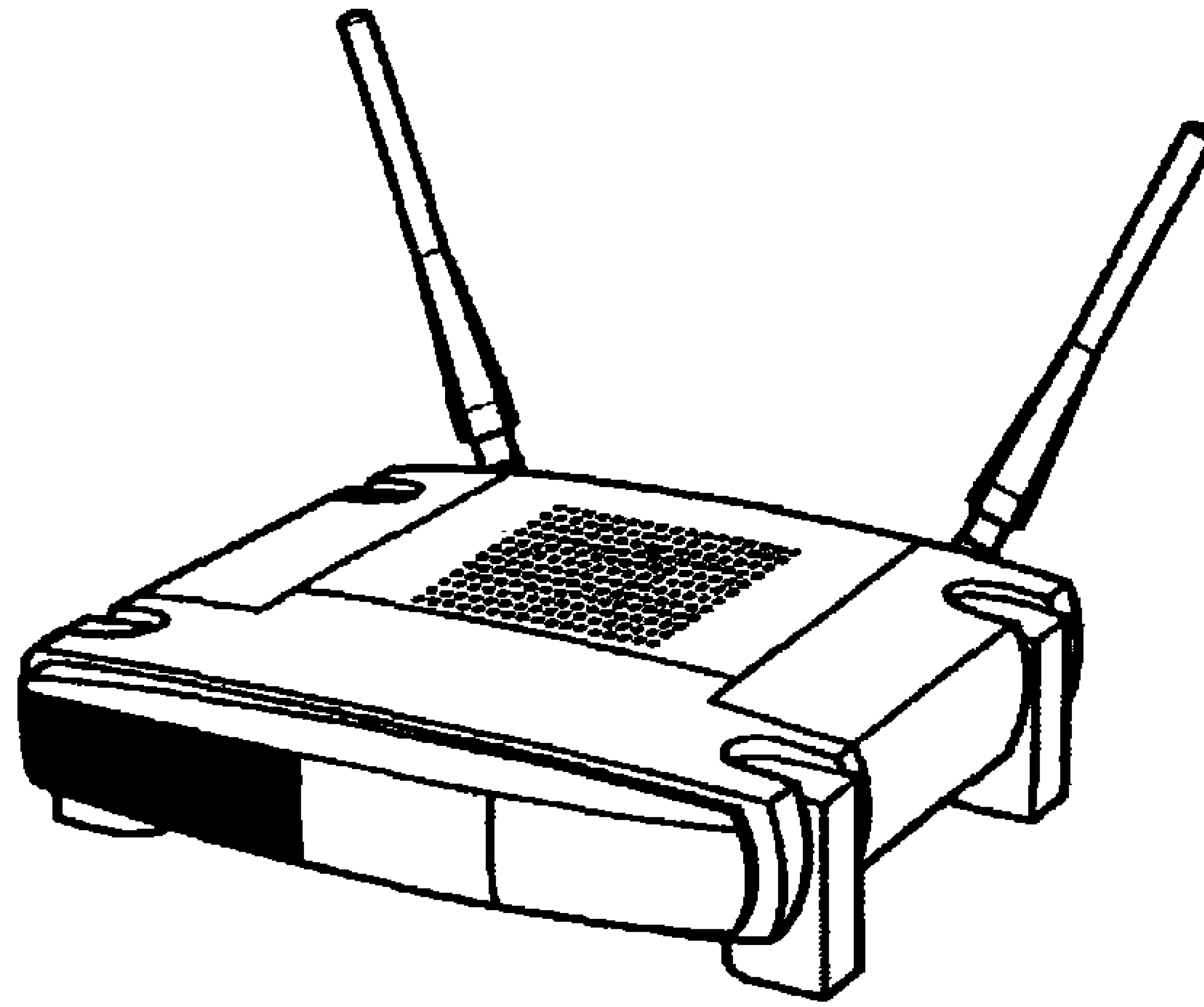
أضخم مصنّعين لوحدات GPS هما Garmin وMagellan. وتقدم كلتا الشركتين نماذج GPS الأساسية والتي تباع بالتجزئة بقيمة 100 دولار أمريكي. ويفضّل المتطفلون لاسلكياً سلسلة النماذج Garmin eTrex بسبب صغر حجمها.

وهناك وحدة GPS مخفية أكثر وهي Sapphire GPS Mouse. تم تصميم هذا المنتج للارتباط بشكل خاص مع حاسب محمول أو مع المساعد الرقمي الشخصي PDA. لكنه ليس متعدد الاستعمالات مثل الوحدات المصممة للتجوال الأرضي أو البحري لأنها لا تملك شاشة عرض أو أزرار تحكم، لكنها أداة مثالية للتطبيقات الخفية تماماً باعتبار قطرها 5 سم فقط.

نقاط الوصول APS: الأدوات السابقة مناسبة للتنصت المتحرك، لكن يمكن أن يستخدم الجاسوس المتطور نقطة وصول AP قياسية لأغراض التجسس (انظر الشكل 6-11). وهناك عدد من الاحتمالات.

إذا كنت تستطيع الوصول فيزيائياً إلى بناء، يمكنك أن تركّب نقطة الوصول AP الخاصة بك على الشبكة المستهدفة، وتعطيك وصولاً عن بعد إلى الشبكة. فعلى سبيل المثال، يستطيع الجاسوس سرياً أن يوصل نقطة وصول AP إلى سدادة بعيدة لشبكة Ethernet متوضعة قرب النافذة مثلاً. ومن ثم بعد أن يغادر المبنى يستطيع توجيه هوائي موجه إلى موقع نقطة الوصول ويتنصت على الشبكة المراقبة باستخدام برنامج sniffer.

طريقة أخرى للهجوم باستخدام نقطة الوصول AP هي وضع نقطة الوصول الخاصة بك والمكونة بشكل مشابه قي مكان ما من الشبكة اللاسلكية WLAN ومراقبة حركة المرور التي تعبرها. مثلاً، يستطيع الجاسوس الداخلي أن يضع نقطة الوصول الخاصة به بين حاسب عميل ونقطة الوصول الأصلية. وبما أن نقطة الوصول المزيفة أقرب من نقطة الوصول الحقيقية سوف يحاول العميل أن يرتبط بنقطة الوصول المزيفة. وسوف يشغّل الجاسوس برنامج sniffer لمراقبة وتسجيل حركة المرور من العميل والمارة بنقطة الوصول الوسطى والتي تسمى في هذه الحالة "man-in-the-middle". خيار آخر للهجوم الوسطي "man-in-the-middle" هو تنفيذ هجوم لتعطيل الخدمة (Denial of Service Attack) ضد نقطة الوصول، ومن ثم استخدام نقطة الوصول الخاصة بك لمعالجة حركة المرور اللاسلكية. (تبدأ أدوات الهجوم لتعطيل الخدمة ضد الشبكات اللاسلكية WLAN بالظهور. وأطلقت مجموعة من البرامج الخدمية للنظام Linux تسمى Air-Jack، في عام 2002 في Las Vegas).



الشكل (6-11) نقطة وصول من تصنيع شركة Linksys، يمكن تثبيتها بشكل سري في الشبكة أو استخدامها في الهجوم الوسطي "man-in-the-middle".

الطائرات، القطارات، والسيارات: ما لم تكن تتنقل مشياً على الأقدام، سوف تحتاج إلى مكان لتنفيذ عمليتك اللاسلكية منه. عندما ترتبط بالتجسس اللاسلكي، سوف تقوم بالاستطلاع المتنقل أو تركّب محطة تجسس ثابتة.

الاستطلاع المتنقل هو ببساطة ما يشير إليه المصطلح "war driving"، أي أنك في الخارج تبحث عن الشبكات اللاسلكية WLAN. قد يكون لديك هدف محدد وأنت مهتم بمعرفة ما إذا تم استخدام الشبكة اللاسلكية WLAN ضمن المبنى، أو ربما تكون انتهازياً وتبحث على بعض الشبكات اللاسلكية غير المؤمنة لتشن هجومك منها.

مثل أي نوع من أنواع التجسس الكلمة المفتاحية هي "غير واضح". أي يتوجب عليك وعلى مركبتك أن تختلطا مع المحيط. مع أنه قد يعشق الجاسوس المؤيد لمذهب حرية التصرف أن يتجادل حول شرعية البحث عن الشبكات اللاسلكية WLAN مع شرطي قد كشفه وقبض عليه، لكن نجاحك يعتمد على الاختلاط وعدم الظهور. أي يجب أن لا تلفت أنت أو سيارتك الانتباه.

بالنسبة للاستطلاع المتنقل فقد تكون وحدك أو مع شريك. إذا كنت لوحدك سوف يكون الحاسب المحمول بقربك على المقعد أو على الأرضية. سوف تمنع قطعة من المطاط غير المنزلق الحاسب المحمول من التحرك كثيراً أثناء القيادة. يرغب المستطلعون "war drivers" أن يشاهدوا نتائج فحص الشبكات اللاسلكية التي تم اكتشافها مباشرة. لكن مع كل الإغراء في معرفة النتائج بسرعة، فمن الأفضل إبقاء غطاء الحاسب المحمول مغلقاً بعد تشغيل برنامج الاكتشاف.

ويجب أن تطّلع على نتائج الاستطلاع بعد أن تنتهي. حيث لن يكون بالأمر الجيد أن تكون مشوشاً بالحاسب المحمول أثناء القيادة، كما يمكن أن تلفت انتباه شرطي المرور أو مشاهد ما، أو يمكن أن تزيد احتمال وقوعك في حادث سير لأنك لا تراقب الطريق.

يمكن تجنب كل هذا بالتعاون مع شريك: سوف يكون الشريك أو الشريكة مسؤولا عن تشغيل الحاسب المحمول وإطلاعك على المعلومات. فإذا كنت رجلاً، تصرف مثل ما تفعل فرق المراقبة المحترفة واستخدم شريكاً من الجنس الآخر. لأن الأزواج لا يلفتون الانتباه مثل رجلين جالسين معاً، أما الفريق الأفضل هو امرأة وطفل. حيث يقوم مرافقك خلال عملية الاستطلاع بتدوين الملاحظات حول الأهداف المحتملة، إما بالكتابة أو بالتسجيل الصوتي.

قبل أن تبدأ بجولتك الاستطلاعية، يجب أن تقضي بعض الوقت لتطلع على الخرائط وتقدر زمن مسارك لكي تتعرف على القضايا التي يمكن أن تؤثر على الاستطلاع. كما يجب ألا تقود بصورة عشوائية، بل استخدم مساراً محدداً مسبقاً لجولتك.

ما هو أفضل وقت لتنفيذ جولتك الاستطلاعية؟ هذا الأمر يعتمد على الهدف. حيث يمكن أن يتم إطفاء نقاط الوصول APs ليلاً بعد الساعة الخامسة مساءً، ولن يتم كشفها باستخدام برمجيات الاكتشاف بعد الانتهاء من ساعات الدوام. من جانب آخر، إذا كان الهدف يملك أمناً للشبكة، قد يكون هناك أحد ما يقوم خلال ساعات العمل بمراقبة وجود أدوات الكشف مثل الأداة NetStumbler. يفضّل معظم المستطلعين "war drivers" القيادة ليلاً، لكن شاشة الحاسب المحمول تضيء السيارة من الداخل وتجعلك مثيراً للشك في هذا الوقت.

القاعدة الأساسية للمراقبة هي التأكد من أن سيارتك نظامية تماماً، وقم دائماً بالالتزام بقوانين المرور. حيث يحب رجال الشرطة استخدام المخالفات كفرصة للتحقق من النشاط المشبوه أكثر. ماذا يحصل لو قبض عليك شرطي مرور أثناء جولتك الاستطلاعية؟ إن معظم رجال شرطة المرور غير مطلعين جيداً على أمور الحاسب ومعظمهم لم يسمع أبداً حول "war driving". يجب أن تكون مهذباً وأن تتعاون، لكن يجب أن تجهز قصة ملفقة لترويها له. يمكنك إخباره أنك تقوم بمسح لقوة إشارة محطة راديو لمشروع مدرسي أو أن هذا عمل استشاري، وهذا ليس بعيداً عن الحقيقة. يمكنك أن تريه الحاسب المحمول ووحدة GPS وتبدأ بالتحدث حول ربح الهوائي، تداخل إشارة الراديو لأجهزة المايكروويف، نسب الإشارة إلى الضجيج، وأمور تقنية أخرى تضمن أن تضجر أي شخص لا يتمتع بهذه المعلومات. لكن أن تقول أنك مستشار أمني حاسبي تقوم بتدقيق للشبكات اللاسلكية لأحد زبائنك، ليس الرد الأفضل في هذه الحالة. حالما يسمع الشرطي كلمة أمن سوف يصبح مهتماً أكثر فأكثر.

النوع الثاني من التحسس اللاسلكي يتضمن استخدام محطة تنصت ثابتة. يمكن أن تستخدم مبنى مكاتب لمراقبة الهدف أو سيارتك كمركز تنصت. بعد أن تم تحديد الشبكة اللاسلكية WLAN، سترغب باستخدام برنامج sniffer إما لجمع الحزم غير المشفرة أو كشف مفتاح WEP. إذا قررت استخدام سيارتك كمحطة تنصت، فإن الجلوس فيها لساعات طويلة وقراءة صحيفة، ليس خياراً ذكياً. سوف تحترق في هذه الحالة (باستخدام لغة الشرطي والجاسوس). حيث من الأفضل أن ترتب تجهيزات المراقبة لكي تتمكن من إيقاف السيارة في مكان ما قرب الهدف ومن ثم الخروج لبرهة.

توجد ثلاثة اعتبارات أساسية لإعداد مركز مراقبة ثابت:

- يجب ألا تثير المركبة أية شكوك وتتناسب مع باقي السيارات في المنطقة. (هذا يعني عدم وجود أية لصاقات على المركبة تدل على "war drivers").
- يجب ألا تكون تجهيزات المراقبة على مرأى واضح، هذا يعني الحاسب المحمول. وهذا أمر هام لمنع الكشف بالإضافة إلى منع سرقة تجهيزاتك. يوجد حلان هما إما وضع الحاسب المحمول في صندوق السيارة أو استخدام شاحنة مقفلة. حيث تشكل الشاحنة المقفلة مع الستائر حلاً مثالياً، لأنه يمكن توجيه هوائي موضوع على مرجل ثلاثي القوام إلى مبنى المكاتب خلال أحد النوافذ.
- هناك الحاجة إلى توفر طاقة كهربائية كافية، لشحن الحاسب المحمول لمدة زمنية أطول عندما تكون المركبة مطفأة. يوجد بديلان إما استخدام بطاريات وصل حمضي ذات نفس الجهد الكهربائي للحاسب المحمول أو أحد أنواع أنظمة الشحن الشمسية.

بالنسبة لمحطات التنصت البعيدة، يمكن أن يُضعف المطر، الثلج، أو الضباب قوة إشارة الشبكات 802.11b. لذلك إذا كان هدفك ليس قريباً، اختر يوماً صافياً لمراقبة الشبكة المطلوبة.

لا تقيد نفسك بالسيارات والشاحنات. في الحقيقة يمكن استخدام أية مركبة للتنصت اللاسلكي. حيث وردت تقارير عن ما يسمى "war-boating" في القنوات، الأنهار، البحيرات، والمدن قرب المرافئ. في أوروبا يتم استخدام القطارات والدراجات أيضاً.

كما أن "war driving" لا تقتصر فقط على الأرض ويمكن أن نسميها "war-flying"، حيث نشر على شبكة الإنترنت أنه تم استخدام طائرات، في شهر آب عام 2002، لاكتشاف الشبكات اللاسلكية WLAN في استراليا والولايات المتحدة. حيث صرح فريق الطيران الاسترالي تحديد أكثر من 95 شبكة لاسلكية أثناء طيرانهم فوق مدينة Perth على ارتفاع 1,500 قدم. أما الأمريكيون فقد أمضوا حوالي الساعة والنصف وهم يحلقون فوق منطقة San Diego واكتشفوا

437 شبكة لاسلكية بينما كانوا يطيرون فوق المناطق المأهولة بالسكان بسرعة أقل بقليل من 140 ميلاً في الساعة، وعلى ارتفاع بين 1,500 و2,500 قدم فوق الأرض. لقد كانت الإحصائيات التي جمعوها شديدة الأثر. حيث أن نسبة 60 بالمائة من نقاط الوصول كانت لا تزال تحوي القيم الافتراضية SSID وفقط 23 بالمائة من الشبكات اللاسلكية WLAN كانت مفعلة تقنية WEP.

البرمجيات

عادة تقوم باستخدام محلل الطيف كأحد أدوات كشف أجهزة المراقبة، وكل شيء مركب ضمن التجهيزات. لكن ماذا حول الشبكات اللاسلكية؟ لقد حصلت على حاسب محمول مع بطاقة شبكة لاسلكية، هوائي مركب داخلياً، ووحدة GPS، لكنك الآن تحتاج إلى البرمجيات لربط جميع هذه التجهيزات معاً لتكتشف الشبكات اللاسلكية لتعرف إذا كانت معرضة للهجوم (بالطبع فإنك لن ترتبط أبداً بتنصت غير شرعي). يحالفك الحظ لأنه هناك عدد من المبرمجين المحترفين من هواة الشبكات اللاسلكية، وقد قاموا بتطوير مستودع حقيقي من الأدوات لكشف الشبكات اللاسلكية WLAN والتنصت عليها. توجد برمجيات تعمل على أنظمة التشغيل Windows، Linux، BSD، Mac، وPocket PC. عموماً يمكن تصنيف الأدوات البرمجية إلى ثلاث فئات.

- أدوات الاكتشاف. تخبرك ببساطة عن وجود شبكة لاسلكية WLAN.
- برامج sniffer. تلتقط حركة المرور الفعلية للشبكة، وتسمح لك بتفحص الحزم.
- أدوات التحويل. تستعرض مواقع الشبكات اللاسلكية WLAN بشكل مرئي.

البعض من هذه الأدوات معقد جداً، لكن حتى لو كنت جاسوساً ذو مهارات تقنية محدودة، يجب أن تقدر على إيجاد برنامج يناسبك. كما أن معظم الأدوات مجانية، لذلك لا تحتاج إلى ميزانية ضخمة.

نعرض فيما يلي شرحاً مختصراً لبعض الأدوات البرمجية الشائعة.

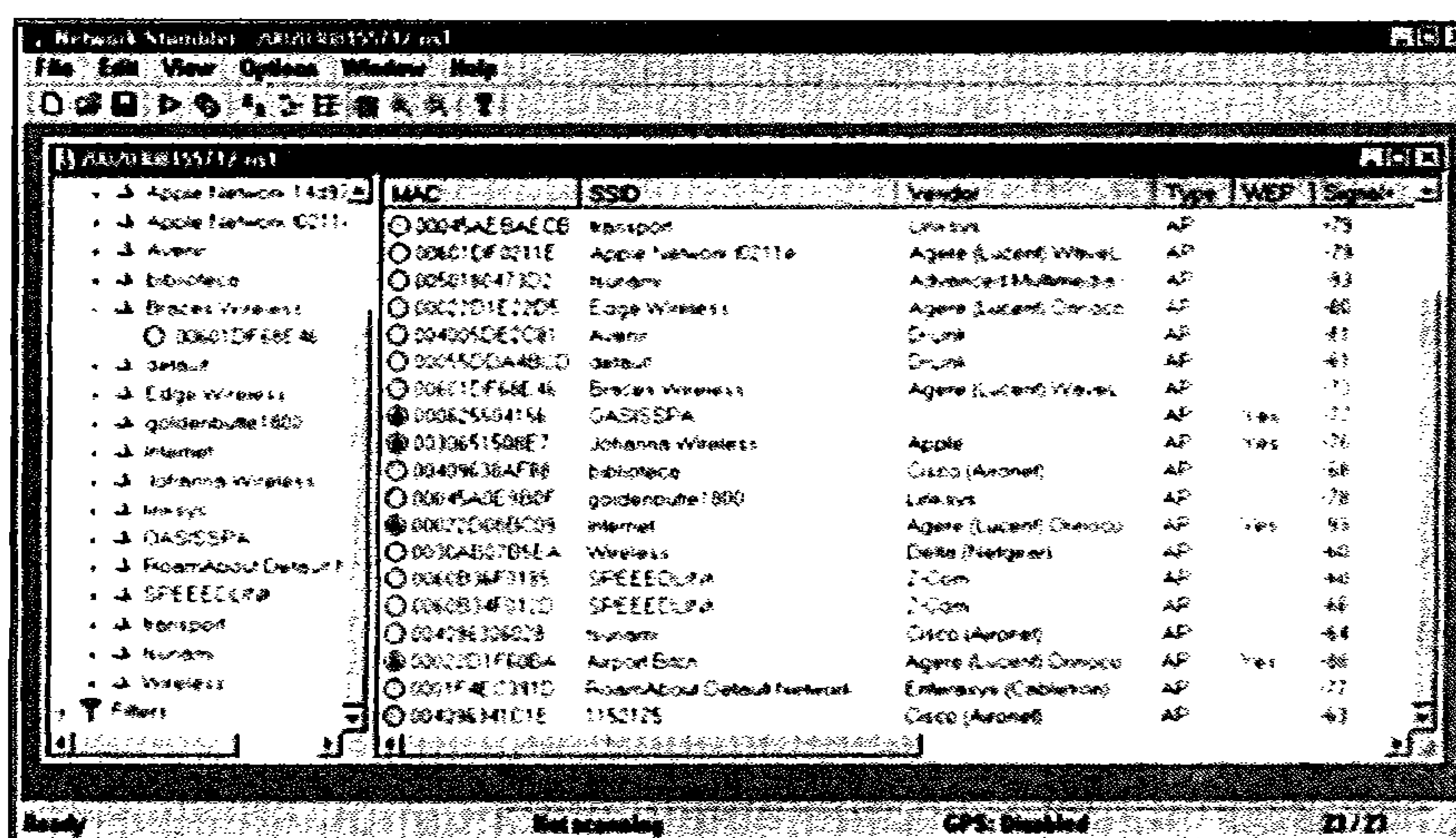
NetStumbler: الأداة Network Stumbler، تسمى غالباً NetStumbler (انظر الشكل 7-11)، وهو برنامج يعمل في نظام التشغيل Windows وهو وراء شعبية ظاهرة "war driving". طوّر هذا البرنامج Marius Milner، وهو موظف في شركة الشبكات اللاسلكية Avaya، يبحث البرنامج NetStumbler عن نقاط الوصول APs. أصدر البرنامج لأول مرة في شهر أيار عام 2001، ومن ثم تحول NetStumbler إلى أداة اكتشاف الشبكات اللاسلكية WLAN متطورة وسهلة الاستخدام جداً.

يعمل برنامج الشبكات اللاسلكية بإرسال سبر بث مرة في كل ثانية، ومن المهم إدراك ذلك لأن NetStumbler لا يعمل بشكل سلبي ويترك علامة عندما يقوم بالسبر. إذا استجابت نقطة وصول، سيحصل البرنامج على قيمة SSID لنقطة الوصول إضافة إلى معلومات أخرى. لا تعد الأداة NetStumbler برنامج sniffer لأنها لا تخزن أو تحلل المجال الكامل لحزم 802.11b والتي تتنقل عبر الشبكة اللاسلكية.

عندما يتم تحديد نقطة الوصول، سوف تسمع صوتاً مفرحاً، وتظهر نقطة الوصول التي تم اكتشافها ضمن اللائحة. تظهر دائرة صغيرة على يسار عنوان MAC وSSID لنقطة الوصول، ويشير لونها إلى قوة الإشارة. وإذا ظهرت أيقونة قفل قرب الدائرة هذا يعني أن تقنية WEP مفعلة. وإذا كانت وحدة GPS موصولة بالحاسب المحمول يتم تسجيل الموقع الجغرافي أيضاً، وهذا ليس الموقع الدقيق لنقطة الوصول إنما النقطة التي كنت فيها عندما اكتشف البرنامج NetStumbler نقطة الوصول هذه.

تم تصميم البرنامج NetStumbler ليعمل مع رقاقات بطاقة واجهة الشبكة Hermes، مثل ORiNOCO، Avaya، وبطاقة الشبكة المحلية اللاسلكية Toshiba. وقد صرح بعض المستخدمون بأنه يمكن تشغيل هذا البرنامج أيضاً مع بطاقات Cisco وبعض أنواع بطاقات Prism-2، إذا كان نظام التشغيل هو نظام Windows XP، مع أنه لم يتم دعمها رسمياً.

إلى جانب إصدار البرنامج الذي يعمل على النظام Windows، طور Milner إصداراً آخر ليعمل على أجهزة Pocket PC مثل Compaq iPAQ.



الشكل (11-7) تُظهر شاشة البرنامج NetStumbler نقاط الوصول المحددة وقوة الإشارة.

لقد نتج عن شعبية برنامج NetStumbler ظهور ثقافة خاصة على الإنترنت. حيث تزود مواقع الويب منتديات للنقاش، الإصدارات البرمجية الحديثة، وقاعدة بيانات يشارك فيها المستخدم لأكثر من 25,000 شبكة لاسلكية WLAN تم اكتشافها. كما أن البرنامج منح مصطلحاً جديداً بديلاً للمصطلح "war driving" وهو "stumbling" وهو يعني أيضاً الخروج بحثاً عن الشبكات اللاسلكية WLAN.



يمكنك تحميل الإصدار الأخير لبرنامج NetStumbler إلى جانب الوصول إلى منتديات النقاش، على الرابط www.netstumbler.com. كما يمكنك زيارة موقع الويب الخاص بالمطور Marius Milner، من خلال الرابط www.stumbler.net.

إن برنامج NetStumbler هو مشروع ثانوي بالنسبة للمطور Milner، ويعمل عليه عندما يتوفر لديه بعض الوقت الإضافي. وهو يعتبر هذه الأداة برنامجاً للمتسولين ويشجع المستخدمين الراضين أن يشاركوا في حسابه PayPal.

KISMET: بالنسبة للأشخاص الذين يفضلون نظام التشغيل Linux، يعد برنامج Kismet خياراً جيداً لاكتشاف الشبكات اللاسلكية WLAN (انظر الشكل 8-11). وبالرغم من أن برنامج NetStumbler شائع ومعروف أكثر، إلا أن برنامج Kismet المجاني والمفتوح المصدر أكثر فعالية من برنامج NetStumbler.

يقوم البرنامج Kismet، على خلاف برنامج NetStumbler والذي يعمل عن طريق إرسال سبر بث، بالتنصت سلبياً على حزم 802.11b ويجمع المعلومات حولها. وبرنامج Kismet جوهرياً هو برنامج sniffer، لأنه سلبي، ولا يمكن كشفه، ويستطيع على خلاف برنامج NetStumbler تحديد موقع نقاط الوصول التي تملك خيار بث SSID غير مفعل.

كما يتمتع برنامج Kismet بعدد من الميزات المفيدة والفعالة مثل التقاط الحزم لعرضها لاحقاً من خلال برنامج Ethereal أو tcpdump، التسجيل المتوافق مع AirSnort، إظهار خرج لبرامج التحويل، والتعرف على مجالات عنوان IP المستخدمة من قبل الشبكة WLAN. كما تتوفر إصدارات هذا البرنامج لأجهزة iPAQ وZaurus المحمولة باليد والتي تعمل على نظام Linux. تم تصميم برنامج Kismet بالأصل ليعمل على بطاقات Prism-2، ولكن هناك ترميمات متوفرة لبطاقات Hermes وAironet.

```
-Networks--(Autofit)-------------------------------------  -Info--
     Name                      T W Ch Packts Flags
 .   St Francis                G N 07    324        0.0.0.0      Ntwrks
     VBHMOUND                  A Y 11     48        0.0.0.0          22
 .   Canhud-POK                G N 06    339        0.0.0.0      Pckets
     <no ssid>                 A N 01   1508 U3     10.132.112.0   6148
     cvsretail                 A N 11   1091        0.0.0.0      Cryptd
 .   IBM-POK                   G Y 00    432        0.0.0.0         386
     peerwap003                A Y 07     56        0.0.0.0        Weak
     linksys                   A Y 06    155        0.0.0.0           0
     <no ssid>                 A Y 11    175        0.0.0.0       Noise
     tsunamisgt3624t           A N 06      4        0.0.0.0           0
     <no ssid>                 A Y 06     58        0.0.0.0      Discrd
     default                   A N 11    284        0.0.0.0        1448
     arlington                 A N 06     15        0.0.0.0
     linksys                   A Y 06     91        0.0.0.0
     LucHomeNet                A Y 06   1107        0.0.0.0
     linksys                   A N 02    107        0.0.0.0
     CPT_Wireless              A N 01    170        0.0.0.0
     WLAN                      A N 11     22        0.0.0.0
                                                                  Elapsed
                                                                  000203
-Status------------------------------------------------------------------
 Detected new network "WaveLAN Network" bssid 00:02:2D:22:86:C1 WEP N Ch 10 @
 Detected new network "WLAN" bssid 00:90:D1:00:09:57 WEP N Ch 11 @ 11.00 mbit
 Detected new network "CPT_Wireless" bssid 00:02:2D:00:04:C0 WEP N Ch 1 @ 11.
 Detected new network "linksys" bssid 00:04:5A:0D:56:0F WEP N Ch 2 @ 11.00 mb
```

الشكل (8-11) تُظهر شاشة برنامج Kismet نقاط الوصول التي تم اكتشافها. وله واجهة نصية، وبالرغم من أن واجهته ليست جميلة مثل واجهة برنامج NetStumbler، إلا أنه أكثر فعالية.



يمكنك تحميل الإصدار الأخير لبرنامج Kismet والحصول على معلومات مفصلة عنه وتعليمات تثبيته، على الرابط www.kismetwireless.net.

حسناً إذا كان برنامج Kismet فعالاً جداً، فلماذا لا يتمتع بنفس القدر من الشعبية مثل برنامج NetStumbler؟ لأنه من السهل جداً تثبيت برنامج NetStumbler ضمن بيئة النظام Windows. بينما يتطلب تثبيت برنامج Kismet جهداً أكبر لأنه يجب أن تتم ترجمته أولاً ومن ثم ربطه بعدد من الحزم التي ليست جزءاً من نسخ Linux الافتراضية. كما أنك تحتاج إلى خبرة تقنية أكثر بكثير لتثبيت البرنامج وتنفيذه.

بالرغم من كمية العمل التي يتطلبها هذا البرنامج، إذا كنت جدياً حول موضوع التجسس اللاسلكي، فهو بالتأكيد يستحق الجهد المبذول بسبب حساسيته الفائقة وخياراته المتقدمة.

برامج sniffer اللاسلكية التجارية والمجانية. "sniffer" هو تسمية أخرى لبروتوكول أو محلل الشبكة الذي يهدف لالتقاط الحزم عندما تتنقل عبر الشبكة. تم تصميم برامج sniffer بالأصل لمساعدة المدراء والتقنيين على إصلاح الخلل في قضايا الأداء في الشبكات لأن برنامج sniffer يستطيع أن يفحص الحزم للبحث عن عدد من المشاكل المختلفة.

أما لأغراض التجسس، فيمكنك أن تستخدم برنامج sniffer لاكتشاف أسماء الحسابات، كلمات المرور، والمعلومات المهمة التي تعبر الشبكة. وبعد أن تلتقط بعض البيانات يمكنك تفحص الحزم لترى إذا كان هناك بعض الأمور المهمة.

تتطلب برامج sniffer كمية معتدلة من الخبرة التقنية لتستخدم بشكل فعال. فهي ليست بسيطة أو بديهية مثل برنامج NetStumbler، ويجب أن تكون على علم بعدة بروتوكولات لكي تفهم محتويات الحزم. فإذا كنت سوف تقوم بكثير من المراقبة اللاسلكية، فمن الجدير بوقتك أن تصبح مستخدماً محترفاً لبرامج sniffer بسبب قوة ضربية كشف المعلومات.

يوجد عدد من برامج sniffer التجارية والمجانية، لنطلع على عدد من برامج sniffer التجارية أولاً:

- **AiroPeek NX**: برنامج sniffer لاسلكي معتمد على النظام Windows لشركة WildPackets. تقوم هذه الأداة بالتقاط وفك تشفير الحزم بنفس الوقت. كما تقدم فك تشفير آني لمفاتيح WEP (لا يخترق برنامج AiroPeek تقنية WEP، يجب أن تزوده بالمفاتيح الصحيحة). لمزيد من المعلومات حول البرنامج، اتبع الرابط www.wildpackets.com/products/airopeek_nx.
- **Sniffer Wireless**: وهو برنامج sniffer آخر من شركة Network Associates. بالرغم من أن هذا البرنامج لا يقوم بفك تشفير حزم البيانات بشكل آني (عليك إيقاف البرنامج أولاً)، لكنه يستطيع فك تشفير عدد هائل من البروتوكولات. كما يتمتع أيضاً بعدد من الخصائص الأمنية مثل قابلية اكتشاف نقاط الوصول المزيفة. لقد ظهرت عائلة برامج sniffer منذ وقت قصير وتوجد غالباً ضمن الإعدادات المغامرة. ولمزيد من المعلومات حول منتج عائلة برامج sniffer، اتبع الرابط www.sniffer.com.

يتم تسويق أدوات sniffer التجارية إلى مدراء الشركات المتحدة والذين يحتاجون إلى إصلاح المشاكل التي قد تظهر في الشبكات لديهم. حيث تتمتع هذه البرامج بعدد من الميزات التي تزيد عن حاجة الجاسوس العادي والذي يبحث فقط عن المعلومات المفيدة، وتعكس كلفتها هذا الأمر. حيث يجب أن تتوقع دفع مبلغ يتراوح من 4,000 إلى 20,000 دولار أمريكي مقابل حزمة برمجية لبرنامج sniffer تجاري.

في معظم الحالات تكون برامج sniffer التجارية ذات آثار تدميرية لأغراض التجسس، ومن الأفضل لك أن تبحث عن برامج مجانية يمكن أن تحملها من شبكة الإنترنت.

يملك مستخدمو نظام Linux عدداً من الخيارات مفتوحة المصدر من ضمنها Kismet، Ethereal (الذي مر معنا في الفصل العاشر)، والتي تستطيع التقاط وعرض حزم البيانات الخام

AirTraf ،Java والمبرمج بلغة (http://chocobospore.org/mognet) MogNet ،802.11b (http://airtraf.sourceforge.net)، و Wellenreiter (www.remote-exploit.org).



لمزيد من المعلومات حول برامج sniffer اللاسلكية للنظام Linux والأدوات الأخرى، اتبع الرابط www.personaltelco.net/index.cgi.WirelessSniffer.

لسوء الحظ إذا كنت مستخدم نظام Windows، لا توجد حالياً أية برامج sniffer لاسلكية ومفتوحة المصدر. لذلك يجب أن تستخدم نظام Linux، أو تشتري أحد المنتجات التجارية.

وسائل التجارة: هل تشكل برامج sniffer تهديداً حقيقياً؟

هل برامج sniffer هي تهديد حقيقي أم نظري فقط؟ بما أن برامج sniffer سلبية، فمن الصعب جداً معرفة إلى أي حد هذا يحدث. فقد لا تعلم شركات الأعمال التي يتم التنصت عليها بهذا، أو إذا اكتشفت اقتحاماً، فقد تختار ألا يتم كشف هذا الأمر بسبب الدعاية السلبية.

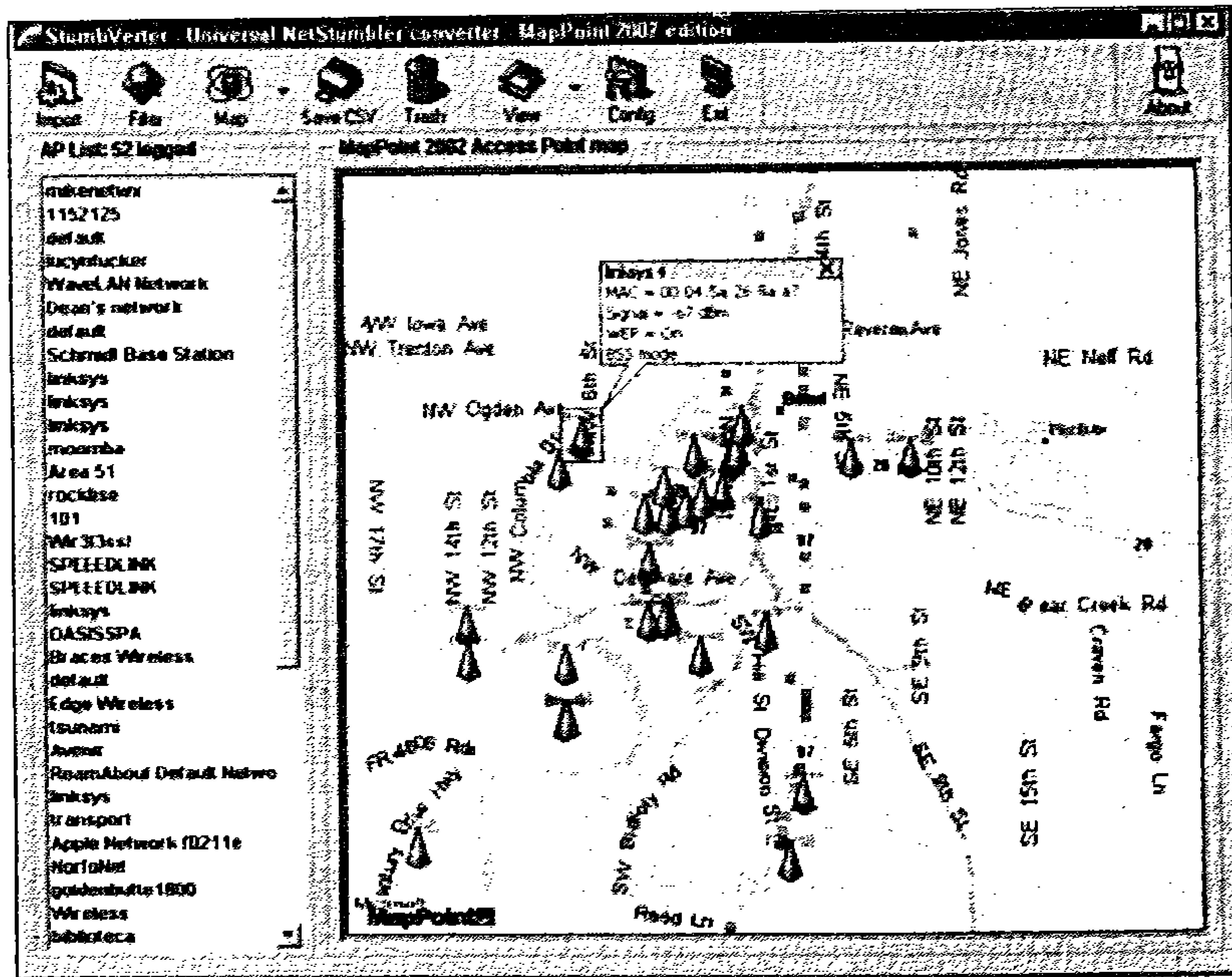
حيث في ربيع عام 2002، ظهر كل من بائع الإلكترونيات بالتجزئة Best Buy و Home Depot في نشرة الأخبار بعد أن تم التنصت على البيانات اللاسلكية عند مواقع التخزين. حيث تنصت "war drivers" المجهزون ببرامج sniffer على مناقلات وقواعد البيانات سجلات النقد اللاسلكي. وقد أعلنت المؤسسة بسرعة أنها قامت بسد جميع الثغرات الأمنية اللاسلكية، ولم يتم كشف أي بيانات للزبائن. وقد ناقض هذا التصريح تقارير مختلفة "war drivers"، بأنه كان يمكن بسهولة معرفة أرقام بطاقات الاعتماد عبر الهواء.

من الهام جداً معرفة أن برامج sniffer اللاسلكية لا تقوم بعرض أسماء الحسابات، كلمات المرور، أرقام بطاقات الاعتماد، والمعلومات القيمة الأخرى بصورة سحرية. حيث يتم تجميع حركة المرور للشبكة، ومع أنه يمكن تطبيق الترشيح، إلا أنه يتوجب على الجاسوس أن يقوم يدوياً باختيار حزم البيانات من بين عدد هائل جداً من الحزم للعثور على أية معلومة قد تكون مفيدة.

تشكل برامج sniffer تهديداً، لكن لكي يتم استخدامها للتجسس يجب أن تلتقط كمية كبيرة جداً من حركة المرور (لأنه إحصائياً تشكل المعلومات المفيدة جزءاً صغيراً جداً من نسبة حركة المرور الكلية). كما يجب أن يتمتع الجاسوس بالصبر ليقوم بفحص جميع المعلومات التي تم تجميعها، ليجد أية معلومات هامة.

AIRSNORT: وهي أداة تعمل على النظام Linux وتقوم بالمراقبة السلبية للإرسالات اللاسلكية المشفرة من أجل اكتشاف مفاتيح WEP. تحتاج هذه الأداة إلى عينة بين خمسة إلى عشرة ملايين حزمة مشفرة (أي ما بين 100MB إلى 1GB من البيانات) قبل أن تكشف المفتاح بنجاح. وقد يستغرق هذا الأمر أياماً أو أسابيعاً. وذلك بحسب حركة المرور للشبكة. بالنسبة لبرنامج Kismet، لا تتوفر الأعداد الثنائية، ويجب ترجمة المصادر – وهذا لا يناسب الجاسوس الذي يستخدم نظام التشغيل Windows ولا يتمتع بخبرة تقنية كافية للنظام Linux. لمزيد من المعلومات اتبع الرابط http://airsnort.shmoo.com.

MAPPOINT: مع أنها ليست أداة لاسلكية، إلا أن برنامج Microsoft MapPoint (انظر الشكل 11-9) وبرمجيات التحويل الأخرى شائعة جداً، لأنها تستطيع الإظهار مرئياً مكان توضع الشبكات اللاسلكية التي تم اكتشافها. يتم الحصول على بيانات الموقع من وحدة GPS واستيرادها إلى برنامج MapPoint من برنامج NetStumbler والأدوات الأخرى من أجل تكوين خريطة.



الشكل (11-9) خرج برنامج **NetStumbler** إلى برنامج **MapPoint 2002** باستخدام الأداة **StumbVerter**

كما يتوفر تطبيق مجاني، مستقل يسمى StumbVerter (www.sonar-security.com) ويقوم مباشرة باستيراد ملفات التلخيص من برنامج NetStumbler إلى برنامج MapPoint. يتم

استعراض نقاط الوصول المكتشفة باستخدام أيقونات خضراء عندما لا تكون تقنية WEP مفعلة، وباستخدام أيقونات حمراء عندما تكون كذلك. يؤدي الضغط على الأيقونة إلى عرض بالون يحوي مزيداً من المعلومات عن نقطة الوصول، ومن ضمنها قيم SSID، عنوان MAC، وقوة الإشارة.

WINDOWS XP: مع أنه قام بعض النقاد بالشكوى من أن نظام التشغيل Windows XP يحوي برامج تجسس داخلية، فإنه يحوي أيضاً وظيفة داخلية مدمجة للتجسس على الشبكات اللاسلكية. افتراضياً، حالما يواجه نظام التشغيل Windows XP بث SSID، سوف يعين النظام آلياً بطاقة واجهة الشبكة إلى نفس قيمة SSID محاولاً الاتصال بالشبكة الجديدة التي تم اكتشافها. هذه ميزة لطيفة جداً للجواسيس غير التقنيين الذين يواجهون شبكة لاسلكية غير محمية. أين تريد أن تتطفل اليوم؟

الإجراءات المضادة

عندما تبحث عن أجهزة المراقبة، فهذا أمر سهل. سوف تجدها وتتخلص منها (أو على الأقل تخبر زبونك أنها موجودة في حالة إذا أراد شن حملة تزييف للمعلومات ضد الأشخاص الذين قاموا بالتجسس عليه). لكن هذه الشبكات اللاسلكية معقدة أكثر بقليل، لأنه حالما أخبرت زبونك بأن شبكته غير محمية، سوف يرغب في معرفة كيف يمكنه حمايتها. وأنت من جهتك، بعد أن تعلمت حول جميع نقاط الضعف لشبكات 802.11b والأدوات التي تقوم باستغلال نقاط الضعف هذه، تتساءل هل كان خياراً صحيحاً أنك تورطت في مجال العمل بأمن الحواسب.

تشجّع. بالرغم من جميع المساوئ الأمنية للشبكات اللاسلكية WLAN، لا يزال بإمكانك دعم الشبكة لمنع أي من المتنصتين أن يتطفلوا من خلال الجو. ومع ذلك لا يوجد حل سحري وحيد يقوم بسد جميع الثغرات معاً. لذلك تحتاج أن تتبع طريقة متعددة الطبقات من الإجراءات المضادة، وتبني كل منها على الأخرى.

افحص شبكتك الخاصة

اجلب نسخة من برنامج NetStumbler أو Kismet لتعرف ما الذي يشاهده الجاسوس عندما يبحث حول مبنى زبونك. اذهب في نزهة بسيارتك مع حاسبك المحمول وهوائي وقم بالتجربة. بسبب سهولة التركيب والسعر المنخفض، يعثر مدراء الشبكة بالصدفة على شبكات لاسلكية داخلية قام الموظفون بإعدادها دون الحصول على الإذن. لا تعتمد فقط على برنامج NetStumbler، فهو محدود بإيجاد نقاط الوصول التي تبث قيم SSID فقط. حيث يقوم برنامج Kismet أو برنامج

sniffer آخر بإيجاد نقاط الوصول الأقل وضوحاً والتي لن يجدها برنامج NetStumbler، ونقاط الوصول هذه هي التي يجب أن تقلق بشأنها.

رتب الهوائيات بشكل صحيح

يجب وضع هوائيات لنقاط الوصول لتقليل فرص تسرب الأمواج الراديوية من الأبنية. تكون نقاط الوصول القريبة من النوافذ أو الجدران الخارجية معرضة للتنصت باستخدام الهوائيات الموجهة نحوها. حيث صرح Shipley في دراسته حول ظاهرة "war driving"، أنه يمكن الوقوف على منحدر التل مع هوائي موجه وتحديد الشبكات على بعد أكثر من 15 كم. ما يجب أن تفعله هو تحسين مكان نقاط الوصول وتعيين الهوائيات الإضافية لتكبير تغطية الشبكة ضمن المكان، مع حصر فرصة وصول الأشعة المباشرة إلى الجاسوس الذي قد يترصد في الخارج.

إجراءات مضادة: AirMagnet

AirMagnet جهاز لإدارة الشبكة اللاسلكية WLAN ويعمل على حاسب الجيب Pocket PC. ويأتي محزوماً ببطاقة لاسلكية خاصة. ومن بعض ميزاته كشف العميل ونقاط الوصول المزيفة، كشف الهجوم لتعطيل الخدمة، كشف تمثيل نقطة الوصول، كشف نقطة الوصول غير المكوّنة، والتقاط وتشفير حزم البيانات في الزمن الحقيقي. تبلغ كلفة جهاز AirMagnet 2,495 دولار أمريكي إضافة إلى كلفة حاسب الجيب Pocket PC. إضافة إلى التدقيقات الإدارية الشرعية، كما يمكن استخدام هذا الجهاز لأغراض التجسس ، اتبع الرابط www.airmagnet.com لمزيد من المعلومات.

إجراءات مضادة: عزيزي، هذا لك

بدأ المقاول الحكومي للمؤسسة العالمية للتطبيقات العلمية SAIC (Science Applications International Cooperation)، في شهر حزيران (يونيو) عام 2002، بمشروع علب حفظ العسل اللاسلكي. أما علب حفظ العسل فهي الشبكات الحاسبية المصممة لإغواء المخرّبين لمهاجمتها ومن ثم تسجيل الطرق التي كانوا يستخدمونها. إن هذه التجربة لأمن المعلومات اللاسلكية متوضعة في موقع آمن في واشنطن، وتملك خمس نقاط وصول من شركة Cisco وسلسلة من الحواسب الشبكية، جميعها تتمتع بالمساوئ المعروفة. كما تمدد الهوائيات كلية الاتجاه للشبكة اللاسلكية WLAN لجذب المتطفلين عن بعد. كما يتعقب نظام كشف اختراق الشبكة IDS وبرمجيات التسجيل أية محاولات للوصول إلى الشبكة.

يملك مستشار KPMG علبة لاسلكية مشابهة لحفظ العسل تعمل خارج رؤسائه في لندن، لمعرفة كمية وقوع ظاهرة "war driving" وتردد محاولات اقتحام الشبكة.

يمكن نصب علب مشابهة لحفظ العسل بسهولة ضمن البيئة المشتركة والتي تعاني من خطر تجسس عالٍ وذلك لمعرفة وجود أية محاولات اختراق نشطة. مع الاهتمام المتزايد بأمن الشبكات اللاسلكية WLAN، على الأغلب سوف تظهر حزم علب عسل لاسلكية تجارية ومفتوحة المصدر في المستقبل القريب.

مع كل هذه المكائد التي يتم نصبها، سوف يخترع مجتمع "war chalking" رمزاً معيناً للمواقع المشبوهة بوجود علب لحفظ العسل.

كشف أدوات اكتشاف الشبكات اللاسلكية

بسبب شعبية الشبكات اللاسلكية 802.11b، تبدأ حزم أنظمة كشف اختراق الشبكات IDS (Intrusion Detection Systems) بإدخال ميزات تكشف المهاجمات اللاسلكية. لن يستطيع نظام كشف اختراق الشبكة كشف وجود برنامج sniffer، لكنه سوف يكشف مهاجمات أكثر نشاطاً حيث يدخل الجاسوس فعلياً إلى شبكتك.

كما ذكرنا سابقاً، فإن برنامج NetStumbler ليس أداة اكتشاف سلبية، وتوجد أدوات جديدة مثل الأداة NSSpyglass التي تعمل على النظام Windows والتي تحذرك إذا قام جاسوس بسبر شبكتك باستخدام البرنامج NetStumbler. لمزيد من المعلومات حول الأداة NSSpyglass، اتبع الرابط http://home.attbi.com/~digitalmatrix/nsspyglass/.

تقدم شركة ناشئة تسمى AirDefense طريقة هجينة أخرى أجهزة/برامج. يتألف نظام شركة AirDefense من حساسات موزعة معتمدة على الراديو تتحسس نقاط الوصول غير المخولة، تقرأ حزم البيانات اللاسلكية، وتصل إلى نقاط الضعف لنقاط الوصول. تستخدم هذه الحساسات خوارزميات وقاعدة بيانات بالمعلومات حول الشبكات اللاسلكية WLAN لكشف وتحليل أية تغييرات في الشبكة ومن ثم تحذير مدراء الشبكة من خط أي مهاجمات. لمزيد من المعلومات اتبع الرابط www.airdefense.net.

أدوات الكشف المزيفة

يوجد إجراء مضاد عسكري إلكتروني تقليدي وهو تشويش العدو بأنه هناك مئات الأهداف على شاشة الرادار بدلاً من هدف أو اثنين. قامت مجموعة Black Alchemy بنفس الشيء

باستخدام أداة مجانية تسمى Fake AP. حيث تبث هذه الأداة معلومات مزيفة إلى برنامج NetStumbler والبرامج الأخرى، وتخدعها بوجود آلاف نقاط الوصول في الجوار. مما يصعّب مهمة الجاسوس كثيراً ليكتشف نقطة الوصول الحقيقية.

تعمل هذه الأداة على منصات النظام Linux، ويمكنك تحميلها من الرابط www.blackalchemy.to.

إجراءات مضادة: أستخدم WEP أم لا أستخدم WEP

شارك "war drivers" من جميع أنحاء العالم، بين 31 من آب و7 من أيلول عام 2002، بالحملة العالمية الأولى لظاهرة "war driving". تم إرسال ملفات التسجيل لبرنامج NetStumbler إلى موقع مركزي لإجراء التحليل. تم اكتشاف حوالي 9,102 شبكة لاسلكية WLAN في أمريكا الشمالية. وتقريباً 70 بالمائة منها لم تكن مفعلة خيار WEP. وهذا يتطابق عموماً مع عمليات المسح الأخرى والتي أظهرت أنه في أي مكان تتراوح نسبة الشبكات التي لا تستخدم خيار WEP من 60 إلى 80 بالمائة.

فإذا كنت مهتماً بأمنك، استخدم تقنية WEP.

تفعيل تقنية WEP

مع أنك قد رأيت أن تقنية WEP غير آمنة، لكنها مع ذلك تزود مستوى أساسي من الحماية للشبكات اللاسلكية WLAN ويجب أن تكون طبقة من طبقات إجراءاتك المضادة. تذكر أن تقنية WEP تحط من أداء الشبكة بسبب تشفير وفك تشفير حزم البيانات. لكن السرعة الأبطأ يقابلها أمن أقوى.

تغيير مفاتيح تقنية WEP بصورة دورية

يجب أن تغير قيمة المفتاح الافتراضية لنقطة الوصول بعد أن تقوم بتفعيل تقنية WEP. تماماً مثل قيم SSID وكلمات المرور، حيث أن المفاتيح الافتراضية معروفة. إلى جانب ذلك، عليك تغيير قيم المفاتيح بصورة دورية. وبالرغم من أنه يمكن اختراق تقنية WEP، لكن توجد أدوات مثل AirSnort والتي تحتاج إلى التقاط كمية كبيرة من البيانات لتستطيع كشف مفتاح WEP بنجاح. وإذا كانت شبكتك تولد كمية كبيرة من حركة المرور، ربما عليك أن تغير قيمة المفتاح أسبوعياً. أما إذا كانت الشبكة تولد كمية قليلة من حركة المرور فقد تستطيع تغيير قيمة المفتاح

شهرياً. قد تكون هذه المهمة الإدارية مستهلكة للوقت في المؤسسات الكبيرة لأنه يجب تغيير جميع المفاتيح على حواسب العملاء أيضاً. كما يجب أن تفعل مع أي إجراء مضاد، قارن دوماً بين التهديد المحتمل مقابل الجهد والسعر.

مصادقة عناوين MAC

تدعم معظم نقاط الوصول ارتباطاً مع لائحة بعناوين MAC مصدقة. فعلى سبيل المثال، إذا لم يكن عنوان MAC لبطاقة شبكة موجوداً ضمن اللائحة، سوف تمنع نقطة الوصول ذلك العميل من الانضمام إلى الشبكة. نظرياً هذا يبدو إجراءاً مضاداً ممتازاً. لكن تقوم برامج sniffer اللاسلكية بكشف عناوين MAC مباشرة لكل من العملاء ونقاط الوصول، وبعد أن تتم معرفة عنوان MAC فمن السهل انتحاله. إلى جانب ذلك، إذا استطاع الجاسوس الوصول فيزيائياً إلى الحاسب المحمول أو حتى بطاقته الشبكية (مثلاً سرقة بطاقة الشبكة من حاسب محمول متروك)، تصبح مصادقة عناوين MAC غير مجدية. وأخيراً يمكن تطبيق هذا الإجراء المضاد ضمن شبكة صغيرة، ولكنه كابوس إداري في مؤسسة ضخمة نتيجة للحاجة المستمرة لضمان تحديث قائمة عناوين MAC.

إعادة تسمية قيمة SSID

يغير بعض مدراء الشبكة مباشرة الاسم الافتراضي لقيمة SSID لنقطة الوصول لديهم، لكنها لا تلعب دوراً كبيراً في مجال الأمن لقيام أدوات مثل NetStumbler بكشف قيمة بث SSID بسهولة إضافة إلى نوع نقطة الوصول AP. إذا غيرت اسم SSID، استخدم اسماً ليبدو مثيراً لاهتمام الجاسوس. مثلاً، RD_LAB.

قد تعتقد أن تغيير اسم SSID لنقطة الوصول باسم افتراضي آخر لمصنّع مختلف يؤدي إلى إرباك الجاسوس. سوف يحاول المتطفل أن يستغل أحد المساوئ المعروفة لنقطة الوصول للمصنّع Cisco لأن اسم SSID لها هو "tsunami"، لكن في الحقيقة هي نقطة وصول مصنّعة من قبل شركة D-Link. مع أن عمليات الخداع الذكية هي إجراءات مضادة جيدة، لكن هذه لن تنجح. حيث تفحص أدوات مثل NetStumbler بث عنوان MAC لنقطة الوصول لتحديد مصنّع الجهاز. حيث تحدد أجزاء من عنوان MAC المصنّع والجهاز. مثلاً، عنوان 00055D-A6F60C MAC، يكون الجزء 00055D هو القسم الأول للأجهزة التي تصنعها شركة D-Link Systems. وبالرغم من أن اسمها "tsunami"، فإن الجزء 00055D يحدد هويتها الحقيقية.

كذلك يقوم برنامج sniffer بكشف قيمة SSID، حتى لو لم يكن خيار بث SSID مفعلاً و لم يتم استخدام تقنية WEP. ويستطيع الجاسوس استخدام قيمة SSID ليحاول الانضمام إلى الشبكة. ويقدم لنا Max Moser، وهو مطور الأداة اللاسلكية للنظام Wellenreiter Linux،هذه النصيحة. يمكن أن يصل اسم SSID إلى 34 محرفاً ويدعم المحارف التي لا يمكن طباعتها، مثل المحرف 7 (BEL) أو 9 (Tab). فإذا استخدمت المحارف التي لا يمكن طباعتها لاسم SSID، فقد لا تستطيع الماسحات وبرامج sniffer عرض الاسم بشكل صحيح.

تعطيل بث SSID

تملك معظم نقاط الوصول خياراً لتعطيل البث لقيمة SSID. فإذا لم يتم بث SSID لن يكتشف برنامج NetStumbler قيمة SSID وبالتالي لن يعرضها. إلى جانب ذلك، لن يستطيع النظام Windows XP أن يكوّن نفسه في محاولة الانضمام إلى الشبكة.

هذا ليس إجراءاً مضاداً سهلاً جداً. أي حالما يتم إقلاع الحاسب أو (في حالة الحاسب المحمول) يتنقل ضمن منطقة التغطية للشبكة اللاسلكية، يتم إرسال إطار للارتباط. تحوي هذه الإطارات دوماً اسم SSID ويمكن عرضها مباشرة من قبل جاسوس يستخدم برنامج sniffer لاسلكي.

تغيير كلمة المرور الافتراضية لنقطة الوصول AP

إذا اكتشف الجاسوس قيمة SSID الافتراضية، فهناك احتمال كبير أن يحاول الوصول إلى نقطة الوصول باستخدام كلمة المرور الإدارية الافتراضية. فإذا نجح في ذلك يمكنه إعادة تكوين شبكتك، وإيجاد ثغرات أمنية أكثر. لذلك يجب تعطيل الإدارة البعيدة، ما لم تحتاج إليها.

استخدام عناوين IP ثابتة مقابل عناوين DHCP

قبل أن يستطيع الحاسب العميل الوصول إلى موارد الشبكة، يحتاج إلى عنوان IP. يعين بروتوكول التكوين الديناميكي للمضيف (DHCP) آلياً عنوان IP للعميل ليصبح نشطاً. يتم استخدام بروتوكول DHCP كثيراً لتسهيل مهام المدير، لكن لسوء الحظ هذا يسهل مهام الجاسوس اللاسلكي أيضاً، والذي يسعى إلى الارتباط بالشبكة WLAN ليتمكن من الوصول إليها، لأنه سوف يتم منح حاسبه المحمول عنوان IP عن طريق البروتوكول DHCP. يجب تعيين عناوين IP ثابتة إلى حواسب العملاء في الشبكات اللاسلكية، مع تعطيل خيار DHCP. وهذا الأمر ليس سهلاً جداً، لأنه قد يحصل الجاسوس على عنوان IP ومن ثم يستخدمه.

تحديد نقاط الوصول خارج تطبيقات جدار الحماية

بسبب نقاط الضعف المتنوعة للشبكات اللاسلكية 802.11b، يجب اعتبار جميع الشبكات اللاسلكية غير موثوقة ويجب ألا يتم تثبيتها خلف تطبيق جدار الحماية. باستخدام هذه الاستراتيجية، إذا كُشفت نقطة الوصول، سوف تكون بقية الشبكة محمية بتطبيق جدار الحماية.

استخدام الشبكة الخاصة الافتراضية Virtual Private Network (VPN)

الشبكة الخاصة الافتراضية VPN هي طريقة للاتصال بشبكة خاصة، مثل الشبكة المحلية في مكتب، من شبكة الإنترنت مثلاً. تشفر الشبكات الخاصة الافتراضية جميع بيانات الشبكة باستخدام تشفير أقوى بكثير من تقنية WEP. يعد استخدام الشبكة الخاصة الافتراضية (VPN) من أحد الإجراءات المضادة الوحيدة الفعالة لتعزيز أمن شبكتك اللاسلكية WLAN.



لمزيد من المعلومات حول الشبكات الخاصة الافتراضية VPN، ارجع إلى الفصل العاشر.

عدم الاعتماد على المسافة البعيدة في الأمن

يعتقد كثير من مدراء الشبكة أن المجال المحدود لشبكات 802.11b هو إجراء أمني بحد ذاته. ومن السهل مراقبة وجود سيارات غريبة ذات هوائيات في الحدائق العامة. من الجدير بالذكر أنه استطاع Pete Shipley الاتصال بشبكة في غربي San Francisco من هضاب أبعد من جامعة California في Berkeley بحوالي 25 كم.

إطفاء نقطة الوصول

يجب أن تطفأ نقطة الوصول دوماً عندما لا يتم استخدامها. فإذا كنت تستخدم شبكتك خلال النهار فقط، عليك إطفاءها ليلاً. فإذا قمت بتعيين ساعات العمل في المكتب، يمكنك ربط نقطة الوصول بمؤقت كهربائي أمني بحيث تقوم بتشغيلها في الصباح وإطفائها في الليل. أحياناً استخدام إجراءات مضادة بسيطة يكون فعالاً بشكل ملحوظ.

تلخيص

إن تهديد التنصت الشبكي اللاسلكي واقعي جداً. حيث استعرض "war drivers" خلال السنوات الماضية أن معظم الشبكات اللاسلكية غير محمية ومعرضة للهجوم. وبالرغم من تغطية وسائل الإعلام الواسعة للقضايا الأمنية، لكن المدراء والمستخدمون لا يزالون يستعملون إعدادات البائع الافتراضية تاركين شبكاتهم معرضة لهجوم الجواسيس.

ومع أن السلوك الإنساني من جانب الأمن سوف يظل تحدياً، إلا أنه من وجهة نظر التقنية سوف يجلب لنا المستقبل أمناً مطوراً أكثر للشبكات اللاسلكية. لقد تم تحديد المساوئ الحالية لشبكات 802.11b، وتظهر المقاييس المعدلة للدفاع.

يعد المعيار 802.11b، الذي يخضع حالياً للمراجعة النهائية، خلَفاً لتقنية WEP. قدمت المجموعة التجارية الصناعية Wi-Fi Alliance (www.wi-fi.org) مواصفات أمنية مؤقتة كخطوة نحو ما يسمى 802.11i ويدعى WPA (Wi-Fi Protected Access). يواجه هذا المعيار كثيراً من الثغرات الموجودة في تقنية WEP، وتم اختبار مواصفات الشهادة في شهر أيار (مايو) عام 2003، مع توفر منتجات WPA في الربع الثالث من السنة.

كما تم تصميم معيار مصادقة منفذ الشبكة 802.1x لتحسين عملية المصادقة في المؤسسات الكبيرة باستخدام ملقم البروتوكول RADIUS (Remote Authentication Dial-in User Service).

وفي الختام، من الجدير تذكر أن التقنية اللاسلكية غير ناضجة قليلاً وهي تمر حالياً بمرحلة المشاكل الأمنية التي مرت بها جميع التقنيات الأخرى. حيث من البديهي أن يتم اكتشاف مساوئ وثغرات وتطوير أدوات جديدة لاستغلال هذه الثغرات. فإذا كنت تدير أو تدعم شبكة لاسلكية، فمن الهام جداً أن تبقى على إطلاع على القضايا الأمنية التي سوف تظهر في السنوات القادمة.



التجسس على الأجهزة الإلكترونية

لا يقتصر التجسس ذو التقانة المتطورة على الحواسب الشخصية فقط. حيث يمكن جمع وتحليل المعلومات من الأعمال والأجهزة الإلكترونية الشخصية. وبالرغم من أن معظم الناس يركزون عادة على تعزيز أمن الحواسب لديهم، إلا أنهم يتجاهلون الأخطار الممكنة الأخرى والتي قد تكشف البيانات الحساسة. نناقش من خلال هذا الفصل أنواع المعلومات التي يمكن استخلاصها من الأجهزة المكتبية الشائعة، أجهزة الاتصالات، الأجهزة الإلكترونية الخاصة بالمستهلك، ويقدم بعض الإجراءات المضادة العملية لتقليل فرص الوقوع ضحية جاسوس. يمكنك أن تجلس وترتاح خلال هذا الفصل ولا تتظاهر بأنك جاسوس كما كنت تفعل في الفصول السابقة، ما عليك سوى أن تتعلم حول التجسس على الأجهزة الإلكترونية.

الأجهزة المكتبية

في الأيام الغابرة عندما كانت الحياة بسيطة أكثر من اليوم، كان الجاسوس يعتمد على الأوراق الكربونية غير المستخدمة أو أشرطة الآلة الكاتبة للحصول على المعلومات حول نوايا الهدف. أما اليوم فإن التجهيزات المكتبية المتطورة معرضة لنفس مقدار الخطر الذي كانت تتعرض له الآلة الكاتبة القديمة عندما يتعلق الأمر بكشف البيانات الحساسة. يجب أن يتم فحص ومراجعة أي جهاز يتعامل مع معلومات هامة أو سرية بحثاً عن نقاط الضعف المحتملة التي يمكن أن يستغلها الجاسوس. من أهم الأجهزة المكتبية التي تتصدر لائحة الأجهزة المعرضة للخطر أجهزة الفاكس وآلات التقطيع.

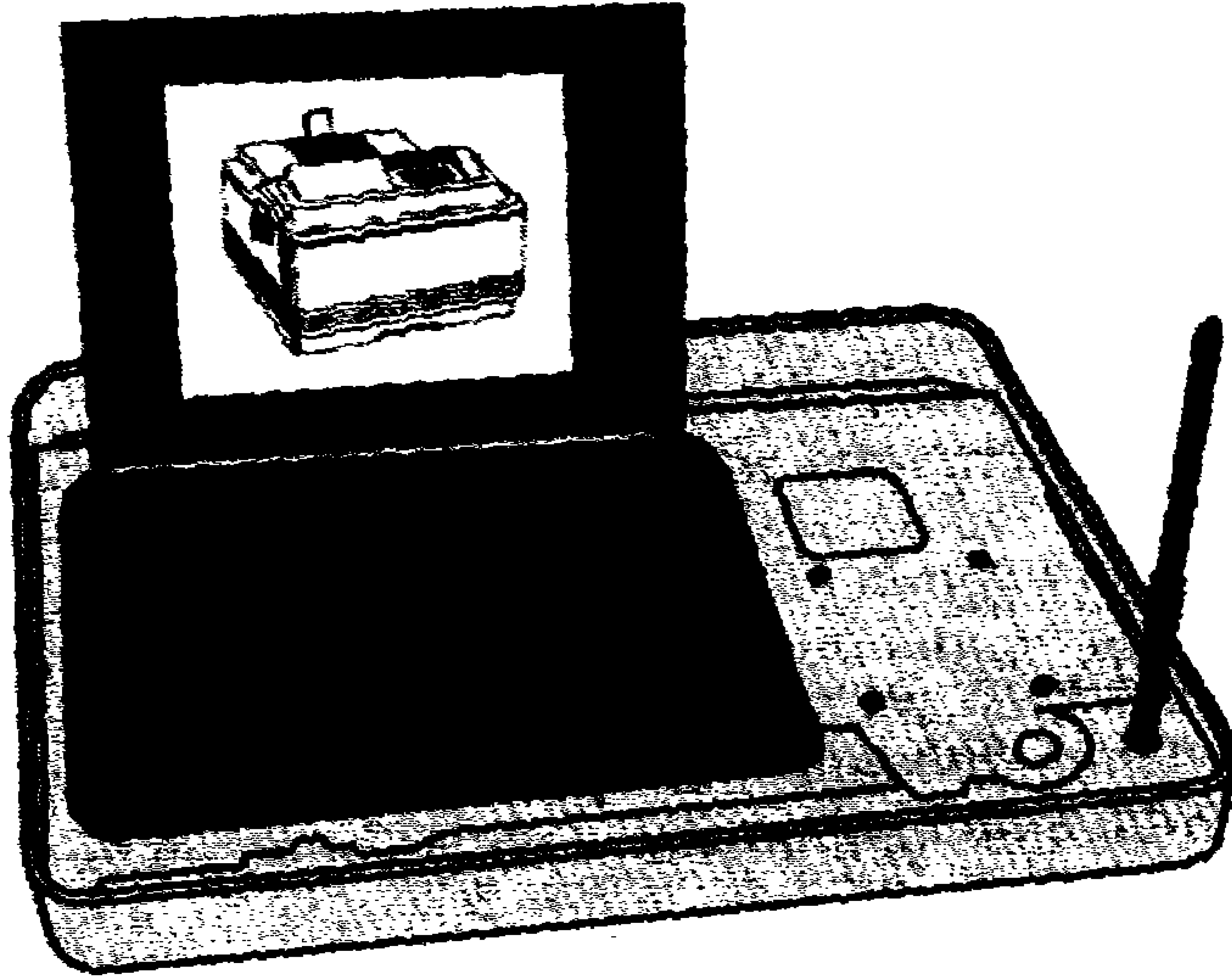
أجهزة الفاكس Fax Machines

كانت أجهزة الفاكس، قبل ظهور البريد الإلكتروني، الطريقة الأساسية لإرسال المستندات بسرعة عبر مسافة طويلة. وبالرغم من أن البريد الإلكتروني، ماسحات الصور، وبروتوكول FTP قد ساهمت جميعها في تضاءل استخدام أجهزة الفاكس، لكنها ما زالت تستخدم بصورة واسعة في المترل، العمل، والحكومة. وبما أنه يتم إرسال المعلومات الحساسة من خلال آلة نسخ، لذلك تشكل أجهزة الفاكس هدفاً أساسياً لعمليات التجسس.

عموماً، توجد أربعة اهتمامات أمنية متعلقة بأجهزة الفاكس، وهي:

- **الاعتراض:** تستخدم أجهزة الفاكس سرعة إرسال منخفضة وبروتوكول موثّق جيداً وغير مشفر لنقل البيانات. بسبب هذا فمن السهل جداً اعتراض إرسال أجهزة الفاكس ومراقبتها. كما تتوفر أجهزة الاعتراض والمراقبة التجارية لأجهزة الفاكس لقوى القانون والوكالات الحكومية لعدد من السنوات (انظر الشكل 1-12 كمثال). فإذا لم يتمكن المتنصت الحصول على أحد هذه الأجهزة، وهي نموذجياً محظور بيعها في الولايات المتحدة، يمكنه أن يتنصت على خط هاتف الفاكس وأن يسجل رقمياً النقل الفعلي على شريط صوتي رقمي DAT (Digital Audio Tape). ومن ثم يقوم بإعادة تشغيله باستخدام جهاز فاكس آخر، جاعلاً جهاز الفاكس يعتقد أنه يتلقى رسالة فاكس من جهاز آخر.
- **لفات الفلم:** تستخدم كثير من أجهزة الفاكس ذات الأوراق البيضاء فلماً كربونياً لطباعة المستندات (هو نفس نوع الفلم المستخدم في خرطوش الآلة الكاتبة الإلكترونية). تحتفظ لفة الفلم الكربونية بصورة مطابقة لكل شيء تمت طباعته. فإذا تم التخلص من لفة الفلم المنتهية أو تم استبدالها من قبل جاسوس يدعي أنه عامل تقني، سوف تظهر صورة واضحة لمحتويات جميع رسائل الفاكس التي استقبلتها. (يمكن استخدام نفس هذا الهجوم ضد أشرطة الآلة الكاتبة والطابعة النقطية).
- **سجلات أجهزة الفاكس:** تحتفظ أجهزة الفاكس أيضاً بسجلات الإرسالات الواردة والصادرة مع معلومات مثل التاريخ، الوقت، عدد الصفحات، وأرقام الهاتف. فإذا استطاع الجاسوس الوصول إلى جهاز الفاكس، يمكن أن يستفيد من هذه المعلومات لتأسيس النماذج والعلاقات.
- **الإرسالات الواردة والصادرة:** خطر كبير عندما تتجمع رسائل الفاكس الواردة ضمن صينية الجهاز على مرأى من الجميع، حتى يصل صاحب الرسالة ويأخذها. أما بالنسبة للإرسالات الصادرة، وقع عدد من الحالات حيث تم إرسال معلومات حساسة إلى الجهة

الخاطئة بسبب طلب رقم هاتف غير صحيح. وبعيداً عن هذه الحوادث، يستطيع الجاسوس تغيير إعدادات جهاز الفاكس أو تعديل التجهيزات الداخلية ليتم إرسال نسخة من جميع رسائل الفاكس الصادرة إلى الجاسوس بشكل سري، على رقم هاتف محدد.



الشكل (12-1) جهاز محمول لمراقبة أجهزة الفاكس، مصنّع من قبل شركة المراقبة البريطانية Eskan Electronics (www.eskan.com)

يوجد عدد من الإجراءات المضادة التي يمكن أن تستخدمها لتحمي نفسك من المتلصصين عندما تستخدم جهاز الفاكس:

- **استخدام جهاز تشفير رسائل الفاكس:** وهو جهاز صغير يصل بين جهاز الفاكس وخط الهاتف ويقوم بتشفير الإرسال. يجب أن يكون لديك جهازان على الأقل: الأول عند جهاز الفاكس المرسل والآخر عند جهاز الفاكس المستقبل (إضافة إلى مقاومة المتنصتين، فإن الأمر الجيد أن الإرسال المشفر لن يتصل بجهاز فاكس لا يملك مثل هذا الجهاز على طرفه). ومن أجل الحصول على أعلى مستوى من الأمن، قم باختيار الجهاز الذي يستخدم خوارزمية تشفير قوية وغير امتلاكية.
- **عدم استخدام أجهزة الفاكس ذات الأفلام الكربونية:** لا تترك أجهزة الفاكس النافثة للحبر أو الحبرية نسخاً مطابقة من رسائل الفاكس التي استلمتها مثلما تفعل الأفلام الكربونية. إما إذا كنت تستخدم فلماً كربونياً عليك تقييد الوصول إلى جهاز الفاكس من قبل الأشخاص غير المخولين وقم بحرق الفلم المستخدم للتخلص منه.

- **عدم إرسال المستندات الحساسة باستخدام أجهزة الفاكس:** قد تكلفك خدمة التوصيل الليلية أكثر بقليل، لكنها عموماً طريقة أكثر أماناً لإرسال المستند. وبدلاً من ذلك، يمكن أن تستخدم تطبيق مثل WinFax Pro من شركة Symantec لمسح سلسلة من المستندات، تخزين ملف الفاكس على القرص الصلب، تشفير الملف باستخدام برنامج PGP أو غيره، ومن ثم إرسال رسالة الفاكس عن طريق البريد الإلكتروني.

أساليب: حيلة النسخ

أصدرت جريدة Popular Science مقالة مشوقة حول كيف استخدمت وكالة الاستخبارات المركزية CIA آلات النسخ المراقَبة للتجسس على الناس في أوائل الستينيات. فصلت هذه المقالة، التي تم تدقيقها بشكل مستقل من قبل عدة مصادر، كيف استطاعت وكالة حكومية استخباراتية تصميم كاميرا مصغرة يمكن زرعها في آلة النسخ. كان الهدف هو سفارة الاتحاد السوفييتي في واشنطن.

عدّل فريق من مهندسي مكنة التصوير كاميرا الأفلام المنزلية باستخدام خلية ضوئية خاصة تقوم بتفعيل الكاميرا حين يتم النسخ. وكانت الكاميرا مخفية في أجزاء من آلات النسخ دون أن تلاحظ. قام التقني بمكنات التصوير بتركيب الكاميرا خلال زيارة التصليح الاعتيادية إلى السفارة السوفييتية عام 1963. وخلال طلب التصليحات تم الحصول على الكاميرا واستبدالها. لقد كانت هناك مؤشرات إلى أن العملية ناجحة جداً إلى درجة أنه تم زرع مثل هذه الآلات في جميع أنحاء العالم.

لا داعي إلى أن تفكر أنه لا يمكن استخدام نفس المراقبة في هذه الأيام، ليس فقط مع آلات التصوير، لكن أيضاً مع أجهزة الفاكس المراقَبة، الماسحات، وآلات التقطيع. وقد لا يحتاج عامل تصليح مكنات التصوير إلى القيام بجولاته الاعتيادية بعد تركيب الجهاز السري، بسبب وجود الكاميرات الرقمية والشبكات اللاسلكية.

آلات التقطيع Shredders

العمل المفضل لدى الجواسيس والمخربين هو التنقيب في المستندات الملقية والتي تم رميها في سلة النفايات. وقد ينتج عن هذه العملية كشف لمختلف أنواع المعلومات الحساسة التي يرميها خارجاً الأشخاص غير المهتمون أو الجاهلون. مفتاح الدفاع لهذا هو استخدام آلة تقطيع: وهو جهاز ميكانيكي يجعل المستندات الورقية غير قابلة للقراءة. (ومع تزايد استخدام الأقراص المضغوطة CD أقراص الفيديو الرقمي DVD لتخزين البيانات، ظهرت آلات التقطيع خاصة في الأسواق في السنوات الماضية وهي تتوفر كوحدات مستقلة أو مدمجة مع آلات التقطيع الورقية).

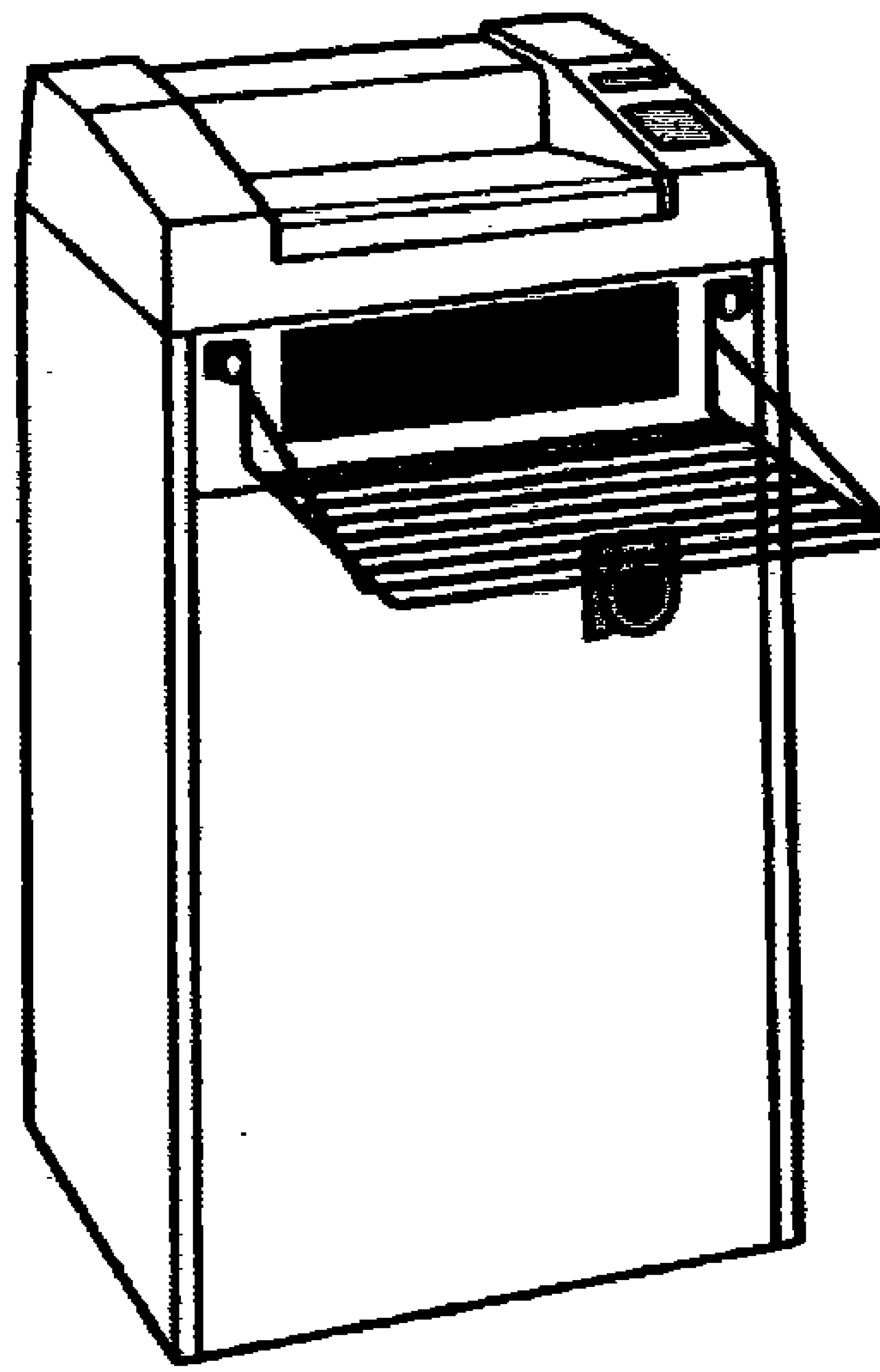
تشكل آلات التقطيع والتخلص من المستندات الحساسة أعمالاً ضخمة، ويقدر أن آلات التقطيع المؤسساتية والحكومية في الولايات المتحدة تولد تقريباً خمسة ملايين طن من بقايا الورق سنوياً. كما تتزايد مبيعات آلات التقطيع الشخصية المنزلية بسرعة لأن الشعب أصبح قلقاً من إمكانية استخدام الورق المرمي في القمامة لتحديد عمليات السرقة.

توجد طرق كثيرة للتخلص من الورق منها التمزيق، الطحن، القص، السحق، والتكسير، لكن الطرق الأكثر استخداماً للتخلص من المستندات المكتبية هي:

- **التفكيك**: تستخدم آلات التقطيع الأقدم هذه الطريقة، والتي تقطّع الورق إلى أشرطة (وبحسب آلة التقطيع، يمكن أن يتراوح عرض الأشرطة الورقية من 12 إلى 4 مم). لا ينصح باستخدام آلات التقطيع التي تستخدم هذه الطريقة للتخلص من البيانات الحساسة، لأنه يمكن ببساطة تجميع الشرطان قرب بعضها وقراءة المعلومات. المثال التقليدي لهذا الأمر هو عندما تم الاستيلاء على السفارة الأمريكية في إيران عام 1979. حيث تم إعادة تجميع مئات المستندات السرية بمشقة كبيرة ونشرها في مجموعة من الكتب بلغ عددها 23 كتاباً وتسمى "Documents from the Den of spies، مستندات من وكر الجواسيس" (اتبع الرابط www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB21/ كمثال). لقد ظن الموظفون في السفارة وفي وكالة الاستخبارات المركزية أن لديهم الوقت الكافي لحرق الأشرطة الممزقة، لكن السفارة سقطت بوقت أسرع مما توقعوه. والسيئة الأخرى للأشرطة الممزقة أنها تحتل حجماً أكبر بسبب حجم الهواء بين القطع. حيث يتم تحويل قدم مكعب واحد من الورق إلى عشر أقدام مكعبة من الورق بعد عملية تفكيكه إلى أشرطة.
- **التمزيق**: هذا النوع من آلات التقطيع أكثر أماناً من النوع السابق لأنها تمزق الورق باتجاه واحد ومن ثم باتجاه آخر، منتجة بذلك قطع ورق صغيرة من الصعب إعادة ترتيبها. نموذجياً، كلما كانت آلة التقطيع مكلفة أكثر، كلما زادت سرعتها وصغر حجم قطع الورق الناتجة. تتراوح أحجام الورق لآلة تقطيع نموذجية من 4×65 مم إلى 0.8×12 مم.

قاعدة الإبهام بالنسبة لآلات التقطيع تقول كلما صغر حجم قطع الورق الممزقة، كلما زاد أمنك. تتطلب وزارة الدفاع الأمريكية أن يتم تقليص المستندات السرية، أو السرية للغاية، أو البالغة الدقة إلى حجم لا يزيد عن 0.8 مم بالعرض و 12 مم بالطول (وللحصول على مزيد من التفاصيل عن التخلص من المستندات السرية راجع مستند برنامج المعلومات الأمنية لقسم الجيش AR 380-5، الملحق K، على الرابط http://ia.gordon.army.mil/iaso/Army/AR%20380-5/AppendixI-K.htm، كما تظهر آلات التقطيع التي تناسب متطلبات NSA/CSS #02-01 في الأسواق والتي تمزق إلى

الحجم 1mm بالعرض و 4mm بالطول. تبلغ كلفة آلة التقطيع العادية التي تناسب مقاييس الحكومة حوالي 800 دولار أمريكي وما فوق). بالطبع فإنك لم تتوقع أن السفارات الحكومية تستخدم آلات التقطيع المكتبية والتي كلفتها 20 دولاراً أمريكياً. من بعض المصنّعين الذين ينتجون آلات تقطيع تتوافق مع المعايير الحكومية تتضمن Dahle (انظر الشكل 2-12)، Intimus، Olympia، و Security Engineered Machinery.



الشكل (2-12) آلة تقطيع Dahle 20634 EC والتي توافق مقاييس NSA وتستطيع تقليص حجم المستندات الورقية إلى قطع بحجم 1mm × 4mm.

هل تحتاج في الواقع إلى آلة تقطيع مصدقة من قبل وزارة الدفاع أو وكالة الأمن القومي؟ يجب أن تأخذ بعين الاعتبار التهديد المحتمل ومن قد يكون مهتماً بكشف بياناتك (كما مر معنا في الفصل الأول). بالتأكيد يجب أن تحصل على نموذج آلة التقطيع التي تمزق الورق، وغير ذلك يجب أن تعرف كمية الورق التي سوف تمزقها يومياً، عدد الأوراق التي يمكنك إدخالها مرة واحدة، وحجم آلة التقطيع.

وإذا أردت ضمان عدم ترك أي معلومات ممكنة للمستندات التي تم تمزيقها، قم بتقطيعها، حرقها، ومن ثم تخلص منها (في المرحاض مثلاً). هذا الأمر تدميري لمعظم الأشخاص، لكن بالنسبة لأولئك الذين يتعاملون مع معلومات بالغة الدقة (أو يملكون أوهاماً بأنهم كذلك)، فهذه الطريقة فعالة جداً.

وسائل التجارة: برمجيات إعادة ترتيب المستندات

إن إعادة ترتيب المستندات الممزقة عمل متعب جداً ويحتاج إلى كثير من الوقت والجهد، وهناك اعتقاد أن وكالات الاستخبارات ووكالات قوى القانون تستخدم عمليات مؤتمتة لاسترداد المعلومات التي تم تمزيقها.

وفي أواخر التسعينيات، قامت شركة تسمى WakeField Integrated Technologies بالإعلان عن تطبيق برمجي يدعى Unshredder، والذي كان يعمل باستخدام ماسحة ضوئية لمسح قطع الورق الممزقة، وبعد الانتهاء من مسح جميع القطع الورقية، استخدم التطبيق خوارزميات التعرف على النماذج لإعادة تجميع المستندات الممزقة.

كان للشركة موقع ويب على الرابط www.unshredder.com والذي كان يعلن عن هذا المنتج، لكن المنتج والشركة اختفيا كلاهما منذ عدة سنوات. والأمر مجهول، هل كانت التقنية غير ناضجة، الموقع كان خدعة، أو قامت وكالة حكومية ما بالاستيلاء على المنتج والتقنية.

(يتمتع Kevin Murray من شركة Murray and Associates، بسمعة طيبة في أعمال مكافحة التجسس، ويملك نسخة حول صناعة تسويق مهنة إعادة بناء الأوراق على موقعه المثقف، www.spybusters.com/pdf/UNshredder.pdf).

أجهزة الاتصالات

يمكن أن يتم كشف المعلومات من أجهزة الاتصالات (مثل الهواتف، الهواتف النقالة، أجهزة النداء، والبريد الصوتي) إما عن بعد (عن طريق التنصت) أو محلياً إذا استطاع الجاسوس الوصول فيزيائياً إلى الجهاز. تعتبر أجهزة الاتصالات تقليدياً أحد أضعف الروابط في الأنظمة الأمنية (الأشخاص مولعون بالأحاديث)، ويمكن أن يتم استغلالهم مباشرة من قبل الجاسوس الذي يحوي التجهيزات التقنية الملائمة. ومن جهة أخرى، إذا كنت تعتقد أن أحداً ما يقوم أو يحاول التنصت على مكالماتك، يمكنك اتخاذ عدد من الإجراءات المضادة لتأمين الاتصالات.

الهواتف Telephones

لقد بدأ التنصت على المكالمات الهاتفية منذ أن بدأت أجهزة الهاتف بالانتشار في أواخر القرن التاسع عشر. حيث استخدم الجواسيس، رجال الشرطة، الأزواج، وغيرهم كل الطرق الممكنة من رفع سماعة هاتف آخر إلى استخدام أجهزة مراقبة متطورة لمراقبة المكالمات الهاتفية بشكل سري. حتى الستينيات من القرن الماضي، كانت أجهزة المراقبة الهاتفية متوفرة من مصادر الطلب

عن طريق البريد لأي شخص تقريباً. ومن ثم قامت القوانين الفدرالية بفرض سيطرتها ومنع استخدام أو تصنيع أجهزة المراقبة الصوتية وحدّت من توفرها إلى وكالات قوى القانون والوكالات الاستخباراتية فقط مع الحصول على أمر من المحكمة يخوّل استخدامها. لكن القوانين لا تنفع كثيراً من أجل منع جاسوس مصمم على التنصت، وخاصة عندما تكون هذه القوانين صعبة التنفيذ والتطبيق، ولا يزال التنصت الهاتفي غير الشرعي تهديداً حقيقياً. (من خارج نطاق هذا الكتاب أن ندخل إلى تفاصيل التنصت عبر الهاتف، تقنيات المراقبة الصوتية، أو الإجراءات المضادة التي يمكن تطبيقها ضدها. وإذا كنت مهتماً بالاطلاع أكثر حول هذا الجانب من التجسس، يمكنك زيارة موقع الويب للخبير التقني Marty Kaiser على الرابط www.martykaiser.com، حيث يعتبر Kaiser أسطورة في أعمال المراقبة وقد قام بتطوير جميع أنواع الأجهزة المشوقة للوكالات الحكومية منذ الستينيات).

عموماً يمكن كشف أجهزة الهاتف لأغراض المراقبة بطريقتين مختلفتين:

- **نقاط التفرع Taps**: يتم التنصت باستخدام طريقة التفريع عن طريق وضع جهاز مراقبة على خط الهاتف. والميزة الأساسية لطريقة التفريع هذه هي أنك لا تحتاج إلى الوصول الفيزيائي للهاتف (أي لا توجد أعمال حقيبة سوداء خطيرة). ويمكن وضع فرع المراقبة على بعد أميال من الهدف. تحدث معظمَ مهام التنصت الشرعية على الهاتف في المكتب المركزي لشركة الهاتف، مما يجعل من الصعب جداً كشفها. (تبيع متاجر الجواسيس أجهزة رخيصة نسبياً لكشف أدوات التنصت، لكنها تعمل ضد أجهزة وتقنيات التنصت الأساسية ولن تجدي نفعاً إذا كان الجاسوس يستخدم تجهيزات متطورة).
- **العثرات Bugs**: إذا تمكن الجاسوس من الوصول فيزيائياً إلى جهاز الهاتف، يمكن تثبيت جهاز مراقبة بداخله. لا تتنصت هذه العثرات على المكالمات الهاتفية فقط، إنما على أية أصوات أو مكالمات تحدث في الغرفة بينما يكون خط الهاتف مفتوحاً. (تحذير سريع لمدراء المكاتب: يمكن لبعض هواتف مكبرات الصوت الجديدة أن تنقل طاقة تردد موجات الراديو التي يمكن اعتراضها على بعد عدة مئات من الأقدام).

بالرغم من وجود كثير من الإجراءات المضادة المتطورة للتغلب على التنصت الهاتفي (سوف نناقشها بعد قليل)، إلا أن طريقة الدفاع الأكثر فعالية هي التكتم وعدم التكلم بالمواضيع الهامة عبر الهاتف.



أجهزة التنصت على الهواتف التجارية والتجهيزات الأخرى المصممة للمراقبة الصوتية السرية غير شرعية في الولايات المتحدة الأمريكية وتتوفر فقط للوكالات الحكومية ووكالات قوى القانون. (لكن توجد شركات مثل Ramsey Electronics، www.ramseykits.com، والتي تقوم بتصنيع أدوات شرعية للأجهزة التي يمكن استخدامها في عمليات المراقبة. كما أن كتاب Winston Arrington بعنوان "How Hear This، كيف أسمع" يتوفر على الرابط www.coverbug.com، مليء بتصاميم لأجهزة المراقبة التي يمكن أن تصنعها في منزلك). للحصول على فكرة حول المنتجات المسموحة للحكومة والممنوعة للآخرين، تحقق من موقع الويب الخاص بمصنّع أجهزة المراقبة Lorraine Electronics في بريطانيا، على الرابط www.lorraine.co.uk.

الهواتف الآمنة SECURE PHONES

إحدى طرق التغلب على التنصت الهاتفي هي استخدام هاتف آمن. لقد ظهرت أجهزة التشفير الصوتية منذ الستينيات، والهاتف الآمن الأكثر استخداماً هو ما تسميه الحكومة بوحدة الهاتف الآمن STU (Secure Telephone Unit). بدأ استخدام وحدات الهاتف الآمن STU في السبعينيات، وهي حالياً في جيلها الثالث (STU-III). يبدو الهاتف STU-III مثل أي هاتف مكتبي آخر (انظر الشكل 3-12) ويعمل مثل الهاتف المكتبي العادي، لكنه يملك ميزة التحدث سرياً مع شخص آخر يستخدم الهاتف STU-III.

ويعمل بالطريقة التالية، تتصل بمستخدم آخر لهاتف STU-III على خط هاتفي عادي ومن ثم تخبره بأن يؤمّن نفسه. أي يقوم المستخدم بإدخال مفتاح خاص (يدعى مفتاح تشغيل التشفير، Crypto Ignition Key، أو CIK) إلى الهاتف. بعد أن يتم إدخال المفتاح ويضغط كلا الطرفين زر Secure Voice (تأمين الصوت)، يتم تشفير محادثتهما. إذا كان خط الهاتف مراقباً، لا يسمع الجاسوس سوى ضجة مشفرة، ويمكن أن تقوم بعض الهواتف الآمنة بتشويه الأصوات والتي قد تبدو بأن شخصاً ما يستنشق الهليوم. عندما تتم إزالة المفاتيح، يعود الحديث إلى كلام عادي غير مشفر. (حالما يتم إدخال المفتاح CIK إلى الهاتف STU-III يصبح جهازاً سرياً، ويتم استخدامه فقط من قبل الأشخاص المخوّل والمسموح لهم استخدامه. عندما تتم إزالة المفتاح يصبح غير سرياً، تبلغ كلفة هذه الأجهزة، التابعة للحكومة، حوالي 3,000 دولار أمريكي وأسعارها تتصاعد).

صرح المرتدون عن خدمات الاستخبارات الأجنبية أن هواتف STU-III فعالة جداً لمنع التنصت. لكن يمكن جمع كمية قليلة من المعلومات من أجزاء المحادثة قبل أن يتم تأمين الهاتف.



الشكل (12-3) إعلان أمني حكومي يظهر هاتف STU-III التقليدي، ونسخة مكبرة من مفتاح تشغيل التشفير CIK ذو الطراز KSD-64A والمستخدم لتهيئة المحادثة الآمنة.



لمزيد من المعلومات عن هواتف STU-III، تحقق من كتيب المستخدم اليدوي الذي نشرته وزارة الدفاع للمقاولين في الوزارة، على الرابط http://koelen.ccc.de/archiv/doku/stu3.pdg. وللحصول على وصف مفصل حول هواتف STU-III (مع الصور) وأجهزة الاتصالات الآمنة الحكومية الأخرى، اتبع الرابط www.tscm.com/stu.html.

بالتأكيد لا تستطيع الخروج إلى السوق وشراء جهاز STU-III، ومع ذلك توجد إصدارات متوفرة للعامة ذات تشفير أضعف. وإذا كنت مواطناً عادياً تريد حماية خصوصيتك، يوجد لديك خياران لإجراء مكالمات هاتفية آمنة.

تبيع معظم متاجر الجواسيس أجهزة لتشويش المكالمات الهاتفية لمنع أحدهم من التنصت بنجاح عليها. تحتاج إلى جهازين: الأول لجهة الإرسال والآخر لجهة الاستقبال. تستخدم أجهزة التشويش الرخيصة تغييراً في التردد لتشويه الكلام (يمكن التغلب على تغيير التردد بسهولة باستخدام أجهزة غير مكلفة والتي تستعيد الأصوات المشوشة إلى كلام مفهوم). تبلغ كلفة الأجهزة غالية الثمن، الموجهة إلى المؤسسات والأفراد الذين يطلبون أمناً أعلى، بحدود 1,500 دولار أمريكي وتستخدم خوارزمية تشفير قوية لتأمين المكالمة.

أعلنت شركة Starium، في عام 1999، بأنها ستزود الشعب بتجهيزات تشفير هاتفية لتأمين المكالمات. كما لاحظ مبرمج خوارزميات التشفير الذي يعمل لصالح الشركة Eric Blossom، أن الجهاز المحمول سوف يباع بسعر التجزئة بحوالي 100 دولار أمريكي، ويتصل بأي جهاز هاتف، ويزود مستوى عالي جداً من الأمن من خلال التشفير القوي (اتبع الرابط www.starium.com/pics.htm). لم يتم إطلاق المنتج أبداً، وكانت حالة الشركة غير مستقرة في نهاية عام 2002، مع وجود احتمال أن يبذل جهد آخر لطرح المنتج في الأسواق.

توجد أيضاً تطبيقات آمنة للصوت فوق بروتوكول IP (VoIP، Voice over Internet Protocol) والتي تقدم بديلاً لإجراء مكالمات هاتفية سهلة الكشف POTS (Plain Old Telephone Service). معظم التطبيقات الصوتية عبر الإنترنت غير آمنة ويمكن التنصت عليها بسهولة، لكن يوجد تطبيقان يقومان بتشفير المكالمات، لمنع محاولات التنصت:

- **Speak Freely**. وهو برنامج خدمي مجاني مفتوح المصدر مطور من قبل Brian C. Wiles وJohn Walker ويعمل على أنظمة التشغيل Windows وLinux. يمكنك تحميله من الرابط www.speakfreely.org.
- **PGPfone**. تم تطوير هذا التطبيق بالأصل لأنظمة Apple Macintosh ومن ثم انتقل إلى النظام Windows. هذا التطبيق مطور من قبل Phil Zimmermann و Will Price، أصبحت هذه الخدمة منتجاً تجارياً عندما اكتسبت شركة Network Associates (NAI) شركة PGP عام 1997. في الحقيقة لم تغير شركة NAI كثيراً في المنتج، وأطلق المبرمج Zimmermann الشيفرة المصدرية له. يتوفر البرنامج على الرابط www.pgpi.org/products/pgpfone.

وسائل التجارة: أجهزة فك التشفير DTMF

الأداة التي لا يمكن أن يستغني عنها الجاسوس للتنصت على الهواتف هي جهاز فك التشفير DTMF، وهو اختصار للعبارة Dual Tone Multi-Frequency. كلما ضغطت على أحد المفاتيح الرقمية لجهاز الهاتف، تقوم بتوليد نغمة فريدة. يقوم جهاز فك التشفير DTMF بتحليل هذه النغمة وإعادتها إلى رقم المفتاح المستخدم لتوليدها.

إذا كنت تملك تسجيلاً للمفاتيح التي تم ضغطها، يمكنك إدخال الصوت إلى جهاز فك التشفير DTMF، ومن ثم تعرض المفاتيح التي ضغطت. وهذا الأمر مفيد جداً لاكتشاف الأرقام التي تم طلبها وكلمات المرور للبريد الصوتي.

يوجد عدد من المنتجات التجارية، غير المكلفة، برمجية وصلبة، لفك التشفير والمتوفرة على شبكة الإنترنت. لمزيد من المعلومات، ابحث ضمن محرك البحث Google عن "DTMF Decoder".

الاختبارات الشرعية الهاتفية PHONE FORENSICS

التنصت على المكالمات الهاتفية ليس الطريقة الوحيدة للحصول على المعلومات من الهاتف. فإذا تمكنت من الوصول إلى الهاتف فيزيائياً، يمكنك الحصول على معلومات مفيدة مما يلي:

- **كاشف الرقم Caller ID**: يعتبر كاشف الرقم ممتازاً لاستعراض المكالمات: عندما يرن الهاتف، يظهر اسم ورقم هاتف الشخص المتصل على الشاشة. كما تقوم أيضاً أجهزة الكاشف، إما أجهزة مستقلة يتم وصلها بجهاز الهاتف أو تكون مركبة داخل الهاتف نفسه، بتخزين سجل بالاتصالات الهاتفية الواردة (سواء أتمت الإجابة عليها أم لا). فإذا لم تقم بحذف الأرقام المخزنة من قبل الكاشف، يستطيع أي شخص أن يستعرض الأرقام التي اتصلت بك. (من وجهة نظر الجاسوس هناك عدد من الطرق للتغلب على أجهزة كشف الأرقام وتجنب عرض رقمك عندما تقوم بالاتصال. اتبع الرابط www.artofhacking.com للحصول على كمية كبيرة من المعلومات حول تجاوز وانتحال جهاز كشف الأرقام).
- **إعادة طلب الرقم الأخير**: تملك الكثير من الهواتف ميزة إعادة طلب الرقم الأخير، حيث يمكنك بالضغط على زر وحيد إعادة الاتصال برقم الهاتف الأخير. هذا الأمر ملائم عندما تتصل برقم هاتف مشغول طوال الوقت، دون أن تكرر طلب الرقم نفسه بشكل متكرر. لكن إذا استطاع الجاسوس الوصول إلى الهاتف، فهذه طريقة لكي يعرف بمن اتصلت آخر مرة. وعند الاتصال، يمكن فك تشفير النغمات باستخدام جهاز DTMF محمول قرب سماعة الهاتف.
- **الاتصال السريع Speed Dial**: أرقام الهواتف المبرمجة مسبقاً للاتصال السريع مفيدة للاتصال بالأشخاص الذين تتحدث معهم معظم الأوقات. كما يستطيع الجاسوس أن يعرف من خلال اللصاقات على الهواتف والأرقام المرتبطة بها، الأشخاص الذين تتكلم معهم.

الهواتف النقالة (الخلوية) Cellular Phones

تشكل الهواتف الخلوية خطراً أمنياً أكبر بكثير من الهاتف الأرضي. بما أن جميع الهواتف الخلوية هي عبارة عن مرسلات ومستقبلات راديو، يمكنك باستخدام التجهيزات الصحيحة التقاط المكالمات من الجو مباشرة دون الحاجة إلى زرع جهاز مراقبة على خط الهاتف، أو حتى القيام بعمل الحقيبة السوداء للوصول إلى جهاز الهاتف فيزيائياً. ويعد هذا النوع من التنصت السلبي صعب الاكتشاف والمنع.

قبل أن ندخل في مناقشة كيفية كشف الهواتف الخلوية لأغراض التجسس. من الهام جداً امتلاك فكرة عامة حول كيفية عمل تقنية الهواتف الخلوية.

تقنية الهواتف الخلوية

شبكات الهاتف الخلوي هي تسمية لسلسلة من الخلايا المرتبطة ببعضها. تملك كل خلية محطة قاعدة (مبنى ذو تجهيزات راديوية وهوائي) تقوم بتأمين التغطية لمنطقة بمساحة عشر أميال مربعة تقريباً.

يدير الحامل الخلوي في المدينة مكتباً مركزياً واحداً يسمى مكتب تحويل الهواتف الخلوية MTSO. يعالج هذا المكتب جميع الاتصالات الهاتفية إلى الأنظمة الهاتفية الأرضية ويتحكم بجميع محطات القاعدة في المنطقة.

يملك كل هاتف خلوي (أو السماعة) رقماً إلكترونياً تسلسلياً ESN (Electronic Serial Number) ورقماً للتعريف المتنقل MIN (Mobile Identification Number) والذي يميز الهاتف بشكل فريد. إذا كان هاتفك يعمل، سوف تمرر هذه المعلومات وغيرها مثل بيانات المصادقة، الصلاحية، والتوجيه جيئة وذهاباً بين هاتفك، محطة القاعدة للخلية التي تتواجد فيها حالياً، ومكتب MTSO. فإذا كنت تتكلم عبر الهاتف وتوجهت نحو طرف الخلية، تتعرف محطة القاعدة بأن قوة إشارتك تنخفض بينما ترى محطة القاعدة المجاورة بأن قوة إشارتك تتزايد، ويتم من خلال مكتب MTSO، تسليم المكالمة من محطة القاعدة الأضعف إلى المحطة الأقوى.

يعتقد معظم الناس أن الهاتف الخلوي هو هاتف خلوي فقط، لكن توجد أنظمة وهواتف خلوية مختلفة والتي تستخدم تقنيات وبروتوكولات متعددة، والتي تسهّل عمل الجاسوس بالتنصت عليك أو تصعبه وذلك بحسب نوعها. تتضمن التقنيات الخلوية الحالية ما يلي:

- **AMPS**: اختصار للعبارة "Advanced Mobile Phone System"، وهي الأنظمة الأولى للهواتف الخلوية في الولايات المتحدة، تستخدم هذه الأنظمة الإشارات التماثلية التي من السهل التنصت عليها باستخدام ماسحة تابعة للشرطة. أوقفت الحكومة، خلال التسعينيات، إنتاج الماسحات التي استطاعت استقبال إرسال بالتردد المخصص للهواتف الخلوية، لكن توجد مصادر كثيرة على شبكة الإنترنت تتضمن معلومات حول كيفية تعديل الماسحات لاستقبال الترددات المحجوبة. تجدر الملاحظة هنا أنه كان من الممكن التنصت على المكالمات التماثلية لأنظمة AMPS باستخدام الماسحات التي يستخدمها المستهلكون بسهولة، بينما لا يمكن فعل ذلك مع التقنيات الرقمية الجديدة للهواتف الخلوية.
- **TDMA (IS-136)**: وهي اختصار للعبارة "Time Division Multiple Access"، تستخدم هذه الأنظمة الإشارات الرقمية والتي تقاوم المتنصتين على الراديو، لكن باستخدامك تجهيزات الاختبار التجارية لهواتف TDMA، تستطيع التنصت على المكالمات الخلوية التي تستخدم هذه التقنية.

- **GSM**: تماماً مثل هواتف TDMA، تحتاج هواتف النظام الشامل للاتصالات النقالة الرقمية GSM (Global System for Mobile Communication) إلى تجهيزات اختبار محددة لمراقبة المكالمات. كما تضيف هواتف GSM طبقة حماية إضافية عن طريق تشفير المكالمات باستخدام خوارزمية تسمى A5.
- **CDMA (IS-95 أو 1xRTT)**: تستخدم هواتف الوصول المتعدد باقتسام الشيفرة ترددات الطيف الضوئي المنتشر الرقمي ، مما يجعل مراقبة المكالمات الهاتفية أمراً صعباً جداً. تحسن الهواتف مثل Qualcomm's NSA-approved QSec-800 الأمن بصورة أكبر عن طريق استخدام تشفير قوي مدمج، واقي TEMPEST، وأختام مقاومة. (للمزيد من المعلومات اتبع الرابط www.qualcomm/com/govsys/pdf/qsec800datasheet.pdf).



لمزيد من المعلومات حول معيار TEMPEST والتنصت الإلكترومغناطيسي، انتقل إلى الفصل الثالث عشر.

ما أريد الإشارة إليه، هو مع وجود كل هذه التقنيات الخلوية المختلفة، هنالك طرق للتنصت على المكالمات. يمكن اعتراض الاتصالات الخلوية في الزمن الحقيقي عن طريق مراقبة الترددات المعروفة، التقاط الإشارات من الجو، ومن ثم إعادة تعديل الإرسال. فإذا كنت تعمل لصالح وكالة قوى قانون وكنت تملك أمراً من المحكمة، يمكنك ببساطة تثبيت جهاز مراقبة في مكتب MTSO.

إذا كنت تعتقد أن هناك شخص ما يلاحقك وقد ينفق الكثير من الموارد من أجل مراقبتك، يجب ألا تعتبر أبداً أن المكالمات الهاتفية آمنة. إذا كنت تستخدم هاتفاً خلوياً تماثلياً، فكن متأكداً أن مكالماتك ستسمع من قبل أي عدد من المتحمسين لأجهزة المسح. يقلص استخدام هاتف رقمي خطر المسح، لكن ما تزال مكالماتك معرضة لمراقبة الوكالات الحكومية ووكالات قوى القانون أو لشخص يتمتع بالتدريب الصحيح والتجهيزات التقنية المناسبة.

بالنسبة للإجراءات المضادة، تملك الحكومة والجيش بعض التقنيات والمنتجات اللاسلكية الأمنية والتي يمكن أن تتعلم عنها من خلال موقع تقنية المعلومات العسكرية، على الرابط www.mit-kmi.com/features/7_1_Art2.cfm. أما إذا لم تكن تعمل لصالح الحكومة وكنت تستخدم النظام الخلوي GSM، يمكنك استعمال الهاتف German TopSec والذي يستخدم تشفيراً قوياً وهو معتمد على هواتف شركة Siemens الشائعة ذات الطراز S35i. لكن لا تتوقع أن تحصل على هاتف مجاناً، من خلال التسجيل على خط خلوي. تكلفة الهاتف أقل بقليل من 3,000 دولار أمريكي، وتحتاج على الأقل إلى جهازين لكي تتمكن من إجراء مكالمة آمنة.



الهواتف اللاسلكية معرضة أيضاً للتنصت، مع أنها تختلف عن الهواتف الخلوية. وتنقل الكثير من النماذج إشارة تماثلية يمكن أن تستقبلها ماسحة راديو. لكن لم يتم حجب الترددات التي تستخدمها الهواتف اللاسلكية من خارج ماسحات التردد الأمريكية، كما هو الأمر مع الهواتف الخلوية، ومع ذلك من غير القانوني مراقبة هذه الترددات. يقدم الهاتف اللاسلكي ذو الطيف المنتشر وتردد 2.4GHz أمناً أكثر بكثير من الهواتف اللاسلكية العادية.

أساليب: التشفير والتنصت الخلوي

تقول صناعة الهواتف الخلوية بأنه لا يمكن التنصت بسهولة على الهواتف الرقمية. هذا صحيح، مقارنة مع الهواتف التماثلية الأقدم، لكن هذا ليس عائقاً أمام الحكومة عندما تمنحك المحكمة أمراً بالوصول إلى مبدّل خلوي لمراقبة مكالمات الهواتف الخلوية.

لنفترض أن الهدف الذي تريد التنصت على مكالماته يستخدم هاتف GSM (لست من وكالة حكومية أو وكالة قوى قانون والتي تستطيع الوصول إلى أجهزة المراقبة التجارية). الشيء الأول الذي سوف تحتاجه هو "مجموعة اختبار الراديو الرقمي، Digital Radio Test Set"، وهي تجهيزات تشخيص واختبار، مصنعة من قبل بعض الشركات مثل Agilent و Racal Instruments، والمصممة خصيصاً لصيانة الهواتف والشبكات الخلوية. تستطيع هذه الأجهزة مراقبة حركة المرور الصوتية وحركة مرور الرسائل SMS ويمكنك شرائها بأقل من 10,000 دولار أمريكي.

لكن حتى لو استطعت أن تراقب الإشارات الرقمية، ماذا عن التشفير الذي يستخدم لحماية حركة المرور؟ لسوء الحظ، فقد تحولت سلسلة خوارزميات "A" المستخدمة لحماية مكالمات GSM إلى خوارزميات ضعيفة جداً، وتم التصريح عن نقاط ضعف متنوعة منذ أواخر التسعينيات، ومن ضمنها ما يلي:

- A5/1: إذا استطعت التقاط البيانات المتعلقة بأول دقيقتين من المكالمة، يمكن اكتشاف مفتاح خوارزمية A5/1 في أقل من ثانية باستخدام حاسب شخصي مكتبي عادي.
- A5/2: وهو أضعف من الخوارزميتين A5 للتشفير الصوتي ويمكن اختراقها بسهولة في الزمن الحقيقي.
- A3 و A8: تستخدم خوارزمية المصادقة A3 لتمنع نسخ الهواتف، أما الخوارزمية A8 فهي خوارزمية السرية الصوتية وتوليد المفتاح، ويمكن أن يتم اختراقها في زمن أقصاه ثمان ساعات.

تم تعريف خوارزمية تشفير GSM جديدة تسمى A5/3، في تموز (يوليو) عام 2002، ومع مرور الوقت يمكننا أن نعرف إذا كانت خوارزمية التشفير هذه تضيف أمناً أكبر لمكالمات الهواتف الخلوية.

هناك اعتقاد، أنه قد احتفظت وكالات الاستخبارات الحكومية على جانبي المحيط الأطلسي والهادي بتشفير الهواتف الخلوية قوياً كفاية لمنع معظم الناس من التنصت على المكالمات، لكن ضعيفاً كفاية لكي تتمكن الحكومة من التنصت على المكالمات.

تحديد موقعك

إذا لم يكن التنصت على مكالماتك سيئاً كفاية، ماذا عن قدرة تعقب آثارك أينما ذهبت؟ من الممكن تحديد موقع الهاتف الخلوي الذي يعمل، عن طريق قياس الوقت الذي تستغرقه الإشارة للوصول إلى محطات القاعدة المحيطة أو عن طريق تحديد الاتجاه الذي تأتي منه الإشارة ومن ثم تثليث موقع الهاتف الخلوي. تستخدم هذه التقنيات في عدة حالات مثلاً لإيجاد وإنقاذ سائقي السيارات المفقودين أثناء العواصف الثلجية. كذلك الأمر تستخدم قوى القانون تقنية تحديد الموقع في التحقيقات الجنائية. حيث استخدم مكتب التحقيقات الفدرالي عام 1995 جهازاً يسمى Triggerfish، مصنّع من قبل شركة Harris Communications، لتعقب المجرم الإلكتروني المطلوب Kevin Mitnick والذي كان يجري مكالمة خلوية في شقته الموجودة ضمن مدينة Raleigh، شمال كاليفورنيا في ذلك الوقت.

سوف يصبح تعقب الهواتف الخلوية أسهل بكثير بالنسبة للحكومة ووكالات قوى القانون. حالما تكون لديك حالة طارئة وتتصل بالرقم 911 من هاتف أرضي، يرى المرسال العنوان الذي تتصل منه. كما تفوّض هيئة الاتصالات الفدرالية نظاماً مشابهاً يسمى 911 المطوَّر (E-911)، والذي بدأ تطبيقه للهواتف الخلوية مع بداية عام 2005. سوف تتضمن الهواتف الخلوية الجديدة وحدات GPS مركبة بداخلها، أو سوف تستخدم الأنظمة الخلوية الموجودة تقنيات تثليث متطورة للقدرة على تحديد موقع الهاتف بدقة. تطالب القواعد المعدلة لهيئة الاتصالات الفدرالية FCC، لأنظمة الشبكات التي تستخدم تقنية التثليث، حوامل الإشارة أن تصل إلى دقة 100 متر لنسبة 67 بالمائة من الاتصالات الطارئة ودقة 300 متر لنسبة 95 بالمائة من جميع هذه الاتصالات. يجب أن تصل دقة الحوامل، التي تقوم بتركيب GPS في الهواتف الخلوية وهذا الأمر أكثر دقة ووثوقية، إلى 50 متر لنسبة 67 بالمائة من الاتصالات الطارئة و 150 متر لنسبة 95 بالمائة من هذه الاتصالات.

الهواتف الخلوية كدليل

إذا كنت تملك وصولاً فيزيائياً إلى هاتف خلوي، فإنه يمكن أن يحوي جميع أنواع المعلومات التي يمكن أن تكون مفيدة إضافة إلى الدليل. (إذا كنت تعمل لصالح قوى القانون وقد أمسكت

بهاتف خلوي، احرص أن تقوم بفحصه بسرعة. لأنه قد يتم تفريغ البطاريات في بعض الأنواع وقد تفقد أرقام الهواتف أو أية بيانات أخرى مخزنة على الهاتف).

سوف يقوم صاحب أي هاتف خلوي يتمتع ببعض الدراية الأمنية، بحماية هاتفه باستخدام رمز أمني. لكن بالنسبة للجاسوس المحترف هذا لن يشكل عائقاً كبيراً ولن يكون سوى تأخير زمني بسيط له، ويختلف هذا الأمر بحسب نوع الهاتف الخلوي. تتوفر رموز فك الحماية والبرمجة بشكل كبير على شبكة الإنترنت لمعظم الهواتف الخلوية الشائعة، وكل ما يجب أن يفعله الجاسوس هو ضغط تسلسل صحيح من الأرقام لفك الحماية عن الهاتف (لتعرف مدى سهولة هذا الأمر، اتبع الرابط www.cellphonehacks.com).

طالما تم فك حماية الهاتف الخلوي، تتضمن المعلومات التي يمكن أن تحصل عليها ما يلي:

- **دليل الهاتف:** تتضمن معظم الهواتف الخلوية ذاكرة لتخزين أرقام الهواتف. وهذا الأمر مفيد جداً للاتصال بسرعة بالأصدقاء، أفراد العائلة، وزملاء العمل كما يخلصك من حاجة أن تحمل دفتر الهواتف معك طوال الوقت. يهتم موظفو قوى القانون بالهواتف الخلوية لأنه إذا كان لديهم أمر من المحكمة، يمكنهم فحص محتويات الهاتف وتجميع الأشخاص المرتبطين بالمشتبه به. قد يشكل الهاتف الخلوي أداة فعالة لتأسيس الروابط في التحقيقات الجنائية.
- **سجل المكالمات:** تتضمن الهواتف الخلوية سجلاً للمكالمات والذي يستعرض الاتصالات المرسلة والمستقبلة من الهاتف، وتحوي رقم الهاتف وزمن وتاريخ الاتصال.
- **معلومات متعلقة بالإنترنت:** دخلت خلال السنوات الماضية ميزات جديدة للهواتف الخلوية مثل البريد الإلكتروني واستعراض صفحات الإنترنت. حيث يمكن استخلاص نفس نوع الدليل الذي نحصل عليه من الحاسب الشخصي من هاتف خلوي يملك ميزة تمكين الإنترنت. وتكون الرسائل الإلكترونية والرسائل القصيرة SMS المخزنة على الهاتف الخلوي، مهمة أيضاً.
- **معلومات متعلقة بالمساعد الرقمي الشخصي PDA:** يوجد اتجاه تسعى إليه الهواتف الخلوية لتضمين كثير من الميزات الموجودة في أجهزة المساعد الرقمي الشخصي. مثل جداول المواعيد، قوائم المهام، وأدلة الهاتف وجميعها تزود معلومات بالغة الدقة للجاسوس.

أجهزة تسجيل المكالمات القادمة Answering Machines والبريد الصوتي Voice-Mail

لقد أصبحت أجهزة تسجيل المكالمات القادمة والبريد الصوتي جزءاً أساسياً من الأعمال اليومية والحياة الشخصية. كما تتوضع هذه الأجهزة والخدمات المناسبة على لائحة الهجوم للجاسوس بسبب المعلومات التي تحويها ولأنها تعتبر نقطة ضعف أمنية محتملة.

نظرياً، تسمح جميع أنظمة البريد الصوتي وأجهزة تسجيل المكالمات القادمة للمستخدم بأن يتحقق ويصل إلى رسائله عن بعد. فإذا استطاع الجاسوس كشف كلمة مرور المستخدم من جهاز هاتف من أي مكان في العالم، يمكنه الاستماع أو حذف جميع الرسائل المتروكة للهدف عن بعد.

يمكن اختراق أنظمة البريد الصوتي وأجهزة تسجيل المكالمات القادمة من خلال عدة طرق:

- **مهاجمات القوة العمياء:** يتكون هذا الهجوم من محاولة تجريب جميع التركيبات الرقمية المحتملة والتي يمكن أن تتألف منها كلمة المرور. حيث يملك جهاز تسجيل المكالمات القادمة الخاص بالمستهلك ذو كلمة المرور المكونة من ثلاثة أرقام، ألف احتمال فقط لكلمة المرور. أما كلمات المرور الخاصة بأنظمة البريد الصوتي التجارية تصل إلى 15 حرفاً. من الواضح أن هجوم القوة العمياء سوف يستغرق الكثير من الوقت، لكن توجد أدوات وبرامج نصية متوفرة تؤتمت هذه العملية، لذلك لا تحتاج لأن تنهك إصبعك وأن تضغط مفاتيح الهاتف.
- **مهاجمات القاموس:** يعتمد هجوم القاموس على سلسلة أرقام محددة مسبقاً ليتم تجريبها ككلمات مرور. قد تكون كلمات مرور افتراضية، كلمات مرور شائعة (التسلسل الشائع مثل 12345، والأرقام التي تتبع نموذج ما مثل شكل حرف "Z" أو "U"، أو نفس أرقام صندوق البريد)، أو كلمات مرور معتمدة على المعلومات الشخصية (أعياد الميلاد، الذكريات السنوية، أو أرقام الضمان الاجتماعي).
- **الهندسة الاجتماعية:** يستطيع الجاسوس من خلال هجوم الهندسة الاجتماعية أن يكشف كلمة المرور وذلك عن طريق السؤال عنها ببساطة (طبعاً مع وجود قصة مقنعة لهذا).
- **الوصول الفيزيائي:** إذا تمكن الجاسوس من الوصول فيزيائياً إلى جهاز تسجيل المكالمات القادمة، يمكن أن تتم طباعة كلمة المرور على لصاقة أو أن تكون مكتوبة في مكان ما قرب الجهاز.

أجهزة تسجيل المكالمات القادمة ANSWERING MACHINES

تشكل أجهزة تسجيل المكالمات القادمة الخاصة بالمستهلك والمستخدمة في المنازل والأعمال الصغيرة هدفاً سهلاً للجاسوس لأن معظمها يملك كلمات مرور مكونة من رقمين أو ثلاثة أرقام فقط. هذا الأمر يجعلها غير آمنة، لأنه يمكن اختراق كلمة المرور المكونة من رقمين خلال خمس دقائق فقط باستخدام هجوم القوة العمياء. بعد أن يصل الجاسوس إلى الجهاز، يمكنه أن يتفقد ويحذف الرسائل، وفي بعض النماذج يمكنه تشغيل الميكروفون للتنصت على المكالمات والأصوات في الغرفة. يبحث عدد من أجهزة التسجيل هذه على تسلسل معين من الأرقام وليس كلمة مرور متميزة. مثلاً يستطيع الجاسوس، من أجل جهاز تسجيل ذو كلمة مرور مكونة من رقمين، أن ينتحل كلمة المرور بإدخال أحد تسلسل الأرقام التالية.

001122334455667788991357902468036925814715937049483827261605173950628408529630074197531864209876543210

12345678987654321357924686429731474193366994488552277539596372582838491817161511026203040506070809001

البريد الصوتي VOICE-MAIL

إن خدمات البريد الصوتي المشتركة أو التابعة لمؤسسة الهاتف معرضة للهجوم تماماً مثل أجهزة التسجيل. وبالرغم من أن أنظمة البريد الصوتي تتمتع بعدد أكبر من الميزات الأمنية، مثل كلمات مرور أطول وإنهاء عملية تسجيل الدخول إذا تم إدخال كلمة المرور بشكل غير صحيح لعدد معين من المرات، لكن توجد بعض الميزات التي تقدم للجاسوس فرصاً أكبر لكشف المعلومات. تمنح أرقام الهواتف المركزية والتي يستطيع المستخدم الوصول إلى بريده الإلكتروني من خلالها دون طلب التمديد للجاسوس رقماً وحيداً والذي يستطيع من خلاله شن مهاجماته على عدة حسابات لصناديق البريد. إلى جانب ذلك، تعمل أنظمة البريد الصوتي المشتركة غالباً بالتعاون مع نظام (تبادل الفرع الخاص PBX، Private Branch Exchange) لنظام الهاتف الخاص بالشركة، وإذا استطاع الجاسوس اختراقه، فإنه يستطيع استخدام نظام PBX لإخفاء أثره من أجل تنفيذ عدد من المهاجمات المختلفة.

تتمتع منتجات البريد الصوتي نموذجياً بعدد من المواصفات الفريدة (مثل التحية) والتي تعطي فكرة للجاسوس عن نوع النظام الذي يتعامل معه، لذلك يمكنها استغلال نقاط الضعف المرتبطة بالنظام (الأوامر وكلمات المرور لعدد من منتجات البريد الصوتي شائعة الاستخدام والمتوفرة على شبكة الإنترنت).

من وجهة نظر الإجراءات المضادة، هناك عدد من الخطوات البسيطة التي يمكن أن تتبعها لتقليص فرص كشف المعلومات من خلال نظام البريد الصوتي أو جهاز التسجيل:

- اختيار كلمة مرور رقمية صعبة (أي لا يمكن توقعها بسهولة) وتأخذ الطول الأعظمي الذي تسمح به الخدمة أو النظام.
- تكوين النظام، في حال كان يدعم هذا الخيار، بحيث يمنع تسجيل الدخول بعد عدد محدد من المحاولات الفاشلة.
- عد ترك معلومات بالغة الدقة على جهاز تسجيل المكالمات أو البريد الصوتي. هذا يعني أنه يجب ألا تترك رسالة تحوي معلومات هامة على البريد الصوتي، وإذا استقبلت رسالة تحوي معلومات هامة يجب أن لا تظل مخزنة على النظام.



يملك Stephan Barnes، (a.k.a "M4phr1k") وهو مستشار أمني لشركة Foundstone، كمية كبيرة من المعلومات عن اختراق ودعم الأمن لنظام PBX و البريد الصوتي على موقعه www.m4phr1k.com. كما تحوي شركة @Stake مقالات مفيدة جداً حول أمن البريد الصوتي كاتبها Joe Grand (a.k.a "Kingpin") بعنوان: "استشارات أمنية حول أجهزة تسجيل المكالمات الهاتفية، "Security Advisory on Telephone Answering Machines (www.atstake.com/research/advisories/1998/ansmach.txt) ومقالة أخرى بعنوان "كشف أنظمة البريد الصوتي ، "Compromising Voice Mail Systems (www.atstake.com/research/reports/acrobat/compromising_voice_mes saging.pdf).

أجهزة النداء Pagers

مع أن أجهزة النداء أصبحت قديمة نوعاً ما ويتم استبدالها بشكل متزايد بالهواتف الخلوية التي تدعم خدمة البريد الإلكتروني وخدمة الرسائل القصيرة SMS، لكنها لا تزال تستخدم بصورة كبيرة ويمكن أن تكون مصدراً للمعلومات والدليل.

تستقبل أجهزة النداء التقليدية الرسائل فقط، بينما تقدم الأجهزة الأحدث مثل Research in Motion (RIM) إمكانيتين. وتماماً مثل أي جهاز آخر يمكن كشف أجهزة النداء أيضاً، عن طريق اعتراض حركة مرور الرسائل أو عن طريق تجميع المعلومات فيزيائياً من الجهاز نفسه.

تستطيع وكالات قوى القانون دوماً الحصول على أمر من المحكمة لشركة أجهزة النداء وذلك لكشف الرسائل التي تم إرسالها إلى جهاز نداء محدد، كما يستطيع الجاسوس أيضاً أن يتنصت على حركة مرور جهاز النداء باستخدام برمجيات وتجهيزات غير مكلفة. (إن التنصت غير المخوّل على أجهزة النداء غير شرعي بموجب عدد من القوانين الفدرالية وقوانين الولاية، لكن من الصعب كشف هذا النوع من التنصت بسبب طبيعته السلبية، مثل المراقبة غير الشرعية للهواتف الخلوية والهواتف اللاسلكية).

جهاز النداء هو عبارة عن مستقبل راديو والرسائل التي يستقبلها يتم إرسالها من البائع كإشارات راديو تماثلية باستخدام بروتوكولات مثل POCSAG (Post Office Code Standardization Advisory Group) أو بروتوكول Flex من شركة Motorola. يملك كل جهاز نداء معرّف خاص يسمى "cap code"، وهو نموذجياً رقم مكون من سبعة أو ثمانية أعداد وهو رقم التعريف الإلكتروني (EIN) للجهاز. يقوم جهاز النداء بالمراقبة المستمرة لتيار الرسائل، وعندما يصادف رسالة تحوي المعرّف "cap code" الخاص به، يقوم بفك تشفير البيانات إلى تنسيق رقمي أو أبجدي ويعرض الرسالة على شاشة بلورية صغيرة.

تجدر الإشارة أنه لا يتم تشفير حركة مرور جهاز النداء، لذا إذا تمكنت من فك تشفير البروتوكول تستطيع قراءة الرسالة (لكن أجهزة RIM BlackBerry تشكل استثناءً، حيث يستخدم جهاز BlackBerry بروتوكولاً رقمياً والذي يتحد مع خوارزمية Triple DES، والتي توفر أمناً جيداً). لكي تستطيع التنصت على رسائل أجهزة النداء التقليدية، تحتاج إلى أربعة أشياء:

- **حاسب شخصي PC**. يعمل على نظام التشغيل Windows.
- **ماسحة Scanner**. يتم استخدام ماسحة راديو لاعتراض الإشارات في مجال التردد المخصص لأجهزة النداء، لا توجد حاجة لتكون الماسحة ممتازة جداً ويمكن أن تكون رخيصة، مثل الماسحات التي يستخدمها رجال الشرطة. تستخدم الماسحات رقاقة مميزة لترشيح الصوت لجعله مناسباً للاستماع من خلال مكبر صوت أو سماعة أذن. لكن لسوء الحظ، لا يناسب الصوت الذي تم ترشيحه كمصدر لفك تشفير رسائل أجهزة النداء. لذلك يجب عليك أن تعدل الماسحة بأخذ فرع من الرقاقة المميزة لكي تتمكن من إرسال البيانات الخام إلى الجهاز المشترك. (هناك مخطط لتطبيق هذا لمعظم أنواع الماسحات إضافة إلى أن الشركات تقوم بإنجاز هذا التعديل إذا لم تكن بارعاً في لحام الحديد).
- **واجهة FSK**. وهي اختصار للعبارة مفتاح الإزاحة الترددية (Frequency Shift Keying). تحتاج الإشارات الصوتية التماثلية لجهاز النداء أن يتم تحويلها إلى تنسيق رقمي للتمكن من عرض نص الرسالة، يتم تحقيق ذلك باستخدام واجهة صلبة تدعم مفتاح الإزاحة الترددية

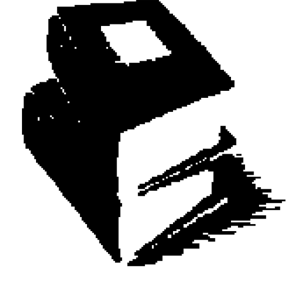
FSK. حيث يتم إرسال دخل الرقاقة المميزة للماسحة إلى واجهة FSK، والتي تقوم بفك تعديل الإشارات الصوتية إلى تنسيق رقمي. (تستطيع بعض البرمجيات تنفيذ فك تشفير محدود للرسائل لكن دون استخدام الواجهة المنفصلة عن طريق استخدام البطاقة الصوتية التي لديك، لكن جهاز الواجهة ضروري جداً إذا كنت جدياً بشأن مراقبة حركة المرور).

- **البرمجيات Software**: تستقبل البرمجيات البيانات المبعوثة من واجهة FSK وتعرضها على شاشة الحاسب. وتوجد بعض الأدوات البرمجية المجانية ونصف المجانية المتطورة والتي تشترك بالميزات مثل اعتراض الرسائل المرسلة إلى جهاز نداء محدد فقط، تسجيل التاريخ والوقت، وإظهار جميع الرسائل ضمن ملف نصي. ومن أشهر البرامج الخدمية المتوفرة على شبكة الإنترنت تتضمن PDW وWinFlex.

مع توفر التجهيزات البرمجية المناسبة، من الممكن صنع " جهاز نداء مستنسخ" والذي يستقبل جميع الرسائل التي يستقبلها جهاز النداء المستهدف. تزود شركات أجهزة النداء هذه الأجهزة لوكالات قوى القانون التي تملك أمراً من المحكمة لمراقبة رسائل المشتبه به. (تشبه المنتجات التجارية للتنصت على أجهزة النداء الإصدارات المترلية المتوفرة لاستخدامات قوى القانون عند إصدار أمر من المحكمة).

كما يجب أن تعلم أنه يمكن كشف رسالة جهاز نداء من طرف الإرسال. فإذا كان خط الهاتف الذي أرسلت منه الرسالة مراقباً، يتم تثبيت لائحة بالأرقام على رقم جهاز النداء، أو إذا تم إرسال الرسالة من موقع ويب أو باستخدام رسالة إلكترونية، يمكن كشف مصدر الرسالة.

أفضل إجراء مضاد يمكنك اتباعه هو ببساطة إدراك أن أية رسالة يتم إرسالها إلى جهاز نداء هناك احتمال أن يتم كشفها. لكن مع ذلك من الممكن التغلب على التنصت على أجهزة النداء باستخدام الرموز (يقوم تجار المخدرات بهذا طوال الوقت). لكن يمكن اختراق الرموز البديلة بسهولة ومن الممكن أيضاً التغلب على الرموز الرقمية عن طريق تحليل حركة المرور إذا كانت هناك حركة مرور كافية لهذا الأمر. ربما أفضل طريقة لتأمين الاتصالات الأبجدية-الرقمية لأجهزة النداء هي استعمال المساعد الرقمي الشخصي الذي ينفذ برنامجاً خدمياً والذي يستخدم خوارزمية تشفير قوية، مثل خوارزميات IDEA، 3DES، أو AES، ومن ثم تشفير الرسالة قبل أن يتم إرسالها. وعندما تصل الرسالة المشفرة إلى جهاز النداء، يدخل المستقبل الرسالة المشفرة إلى جهاز المساعد الرقمي الشخصي الخاص به ومن ثم يفك تشفيرها باستخدام كلمة مرور مسبقة. بالرغم من أن هذه الطريقة مستهلكة للوقت كثيراً وليست بسيطة، إلا أنها فعالة إذا تم استعمال كلمة مرور قوية.



توجد كثير من المعلومات على شبكة الإنترنت حول فك تشفير رسائل أجهزة النداء. قم بالبحث في محرك البحث Google عن "POCSAG decoder"، وتظهر لك عدد من الروابط. أما بالنسبة للمبتدئين، قد تفضل تجربة موقع Mike ZL3TMB's POCSAG والذي يعرض عدداً من البرامج الخدمية لفك تشفير رسائل أجهزة النداء (http://homepages.ihug.co.nz/~Sbarnes/pocsag/software.html). وإذا كنت تميل إلى الإلكترونيات، يتضمن موقع Libor Ulcak رسوماً تخطيطية لتجهيزات صلبة لصنع جهاز لفك تشفير جهاز النداء (www.applet.cz/~ulcak/4_level_fsk_interface.htm).

علاوة على مراقبة أجهزة النداء، إذا كنت تملك وصولاً فيزيائياً إلى الجهاز يمكنك كذلك استخلاص معلومات مفيدة، ومن ضمنها ما يلي:

- الرسائل الأبجدية-الرقمية المخزنة وغير المحذوفة.
- متى وكيف تم إرسال الصفحات الأبجدية-الرقمية عبر (البريد الإلكتروني، موقع الويب، والهاتف).
- المعلومات الرقمية (أرقام الهواتف والرموز).

هناك نوعان من أجهزة النداء الأحدث مثل Black Berry لشركة RIM (ويمكن تصنيفه بين جهاز النداء والمساعد الرقمي الشخصي اللاسلكي)، وهذه الأجهزة أعقد بكثير للفحص. ألف Michael Burnette مقالة ممتازة تسمى "الاختبارات الشرعية للجهاز اللاسلكي RIM (Black Berry)، (Forensic Examination of a RIM (Black Berry" (متوفرة على الرابط www.rh-law.com/ediscovery/Blackberry.pdf)، وتتحدث المقالة عن بعض التحديات والتقنيات لتجميع الأدلة من جهاز Black Berry.

إلكترونيات المستهلك

لقد اعتاد التجسس الحاسبي والاختبارات الشرعية الحاسبية أن تكون بسيطة للغاية، لأنك قد تبحث عن المعلومات أو الدليل على القرص الصلب للحاسب، الأقراص المرنة، أو أية وسائط تخزين أخرى قد تكون بالجوار. لكن من جهة ثانية جعلت شعبية الأجهزة الإلكترونية المستهلكة البحث عن المعلومات عملية معقدة. حيث أن أجهزة المساعد الرقمي الشخصي PDA شائعة بشكل كبير وتتطلب طريقة أخرى للبحث عن البيانات. إضافة إلى ذلك يمكنك حالياً إخفاء البيانات في جميع أنواع الأجهزة الإلكترونية المختلفة، ومن ضمنها منتجات المستهلك المصممة

بصورة أساسية لالتقاط الصور، تشغيل الموسيقى، أو تسجيل البرامج التلفزيونية. وقد يخفي المستخدمون الخبراء تقنياً المعلومات ضمن أحد هذه الأجهزة وقد لا تتم ملاحظتها أثناء البحث. وهذا الأمر يشكل تحدياً للفاحصين الحكوميين أو الذين يعملون لصالح وكالات قوى القانون مما يجبرهم على توسيع معلوماتهم التقنية خارج نطاق الحواسب التقليدية إلى جانب تطوير أدوات وطرق جديدة لمعالجة الأدلة الرقمية في الاختبارات الشرعية، والتي قد تكون موجودة في منتجات المستهلك الإلكترونية.

أجهزة المساعد الرقمي الشخصي PDAs

إن أجهزة المساعد الرقمي الشخصي شائعة جداً، ويعود نجاحها إلى قدرتها على تخزين معلومات المتصلين، المواعيد، السجلات المالية، أوراق العمل، والمستندات النصية ضمن منصة محمولة يمكن أخذها إلى أي مكان تريده. ويقدر أنه تم بيع أكثر من عشرين مليون جهاز رقمي شخصي PDA في السنوات الخمسة الماضية.

كما قد توقعت، تشكل أجهزة المساعد الرقمي الشخصي هدفاً مفضلاً للمتلصصين المهتمين بالمعلومات التي يحتويها الجهاز. لكن بسبب صغر حجمها، يمكن إضاعة الجهاز أو أن تتم سرقته. ففي التقرير الذي نشرته شركةGartner Group في كانون الثاني عام 2002، سلطت الشركة الضوء على أنه سوف تتم سرقة حوالي 250,000 جهاز PDA وهاتف خلوي في المطارات سنوياً. كما نشرت مجموعة الأبحاث الاستشارية Anderson Consulting في نهاية عام 2001 نشرة تقدر بأنه سوف تضيع أو تُسرق في النهاية نسبة 10 إلى 15 بالمائة من الهواتف الخلوية و أجهزة المساعد الرقمي الشخصي PDA. قد تعتقد أنه ليس أمراً مهماً أن تتم سرقة قطعة صلبة سعرها حوالي مائتي دولار أمريكي، لكن صرحت النشرة كذلك أنه تبلغ قيمة المعلومات المخزنة داخل هذه الأجهزة ما بين 10,000 و20,000 دولار أمريكي. (فإذا كنت تملك جهاز PDA، فكر بقيمة جميع الأسماء، العناوين، أرقام الهواتف، المواعيد، الرسائل الإلكترونية، والملفات الأخرى الموجودة في الجهاز).

سوف نركز على الحالة التي يكون فيها أحدهم مهتماً بالمعلومات المخزنة على جهاز PDA أكثر من الجهاز نفسه. ومن بعض الطرق التي يمكن بوساطتها كشف المعلومات تتضمن ما يلي:

- **الممارسات الأمنية السيئة للمستخدم:** تتضمن معظم أجهزة المساعد الرقمي الشخصي أحد أشكال المصادقة باستخدام كلمة المرور من أجل حماية البيانات، لكن الكثير من المستخدمين لا يستعملون هذه الخاصية، مما يسهل مهمة الجاسوس الذي يملك الوصول الفيزيائي للجهاز للحصول على جميع أنواع المعلومات.

- **التشفير الضعيف:** حتى عندما يتم استخدام نظام المصادقة الخاص بالمصنّع، لا يزال ممكناً أن يكون سيئاً. فعلى سبيل المثال، تم اكتشاف أن المخطط المستخدم لحماية مستندات نظام التشغيل Palm والمحددة بأنها مستندات خاصة "Private"، أنه بكل بساطة خوارزمية XOR والتي يمكن اختراقها بسهولة في غضون ثوانٍ (اتبع الرابط www.atstake.com/research/advisories/2000/a092600-1.txt).

- **التزامن:** وهو عملية تبادل البيانات بين حاسب شخصي وجهاز المساعد الرقمي الشخصي: يتم نقل البيانات بين الجهازين باستخدام كبل موصول بمنفذ USB أو المنفذ التسلسلي للحاسب الشخصي. وعندما يحصل التزامن تتم مضاعفة البيانات المخزنة على جهاز المساعد الرقمي الشخصي على القرص الصلب للحاسب. وبالتالي أي شخص يستطيع الوصول إلى الحاسب يمكنه تفحص هذه الملفات (ومن بينها استرداد كلمة المرور) أو نسخ جهاز PDA المضاعَف عن طريق إيداع الملفات إلى جهاز PDA مشابه. كما يمكن أيضاً مهاجمة أجهزة المساعد الرقمي الشخصي عن بعد عن طريق التزامن مع منفذ الأشعة تحت الحمراء. وقد أطلقت شركة Stake@ أداة تعمل على نظام التشغيل Palm وتسمى NotSync (www.atstake.com/research/advisories/2000/notsync.zip) والتي تؤسس محادثة عن طريق الأشعة تحت الحمراء مع نظام تشغيل آخر من النوع Palm ويجعله يظن بأنه يتزامن مع حاسب شخصي. ومن ثم تنتزع هذه الأداة كلمة المرور للجهاز PDA وتقوم بفك تشفيرها.

- **تفريغ الذاكرة إلى ملف:** إذا كنت تملك وصولاً فيزيائياً إلى جهاز PDA، فإنه من السهل نسبياً أن تقوم بتفريغ كامل المحتويات إلى القرص الصلب للحاسب، حيث يتم تفحص والبحث في البيانات. ومن السهل جداً تفريغ محتويات الذاكرة لأجهزة PDA ذات نظام التشغيل Palm باستخدام أدوات مثل pdd (www.mindspring.com/~jgrand/pdd/).



في نهاية عام 2002، تصدرت أجهزة المساعد الرقمي الشخصي حصتها من السوق بنسبة 65 بالمائة في الولايات المتحدة، بالرغم من إدراك حاسب الجيب Pocket PC أيضاً لشركة Microsoft بنسبة كبيرة من السوق، فإذا صادفت جهاز PDA من المحتمل أن يكون ذو نظام التشغيل Palm. وبالنسبة للجواسيس والفاحصين الشرعيين الذين يتوقون إلى استخراج المعلومات من نظام Palm، يمكنهم أن يبدؤوا بمكان جيد للإطلاع وهو المقالة التي ألفها Joe Grand بعنوان"pdd: مضاعفة الذاكرة والتحليل الشرعي لأجهزة نظام التشغيل Palm، " pdd: Memory Imaging and Forensic Analysis of Palm OS Devices على الرابط (www.mindspring.com/~jgrand/pdd/pdd-palm-forensics.pdf).

كما يمكنك أيضاً التحقق من منتج شركة Paraben للحصول على أجهزة PDA، وهو برنامج خدمي لاكتساب وتفحص محتويات كل من أجهزة حواسب الجيب Pocket PC وأنظمة Palm OS. تكلفة الأداة 199 دولار أمريكي (تبيع الشركة أيضاً مجموعة كاملة من الكبلات والمحولات لتجميع الدليل من ثلاثين نوعاً مختلفاً من أجهزة PDA)، لمزيد من المعلومات اتبع الرابط www.paraben-forensics.com/pda.html.

إن الإجراء المضاد الأول ضد التجسس على أجهزة PDA هو الحذر وإدراك قيمة المعلومات المخزنة على جهاز PDA واتخاذ الإجراءات الضرورية لحماية الجهاز فيزيائياً من السرقة أو الضياع. أما الميزات الأمنية القياسية الموجودة ضمن الجهاز فهي غير ملائمة لتزويد مستوى حماية عالي ضد الجواسيس. لذلك فإن الخيار الأفضل هو استخدام تطبيق تشفير من طرف ثالث لتأمين جهاز PDA بشكل أفضل. بعض الخيارات الممكنة تتضمن ما يلي:

- **PDA Defense**: يستخدم لأجهزة Palm وحواسب الجيب، سعره 29.95 دولاراً أمريكياً، ويتوفر على الرابط www.pdadefense.com.
- **Sentry 2020**: متوفر لحواسب الجيب بسعر 49.95 دولاراً أمريكياً، مع بعض المعلومات على الرابط www.softwinter.com/sentry_ce.html.
- **OnlyMe**: تطبيق أمني لأجهزة Palm على الرابط www.tranzoa.com، كلفتها 9.95 دولاراً أمريكياً.
- **TealLock**: تطبيق أمني متوافق مع أجهزة Palm كلفة الإصدار الشخصي 16.95 دولار أمريكي والإصدارات المؤسساتية 21.95 دولاراً أمريكياً، ويتوفر على الرابط www.tealpoint.com/softlock.htm.

الكاميرات الرقمية Digital Cameras

لا تقتصر عملية البحث عن المعلومات ضمن الكاميرات الرقمية على مجرد تقليب الصور التي تم التقاطها، وبعض الأمور الواجب معرفتها عند البحث عن المعلومات أو الأدلة في الكاميرات الرقمية تتضمن ما يلي:

- يدعم التنسيق JPEG إرفاق كميات نصية صغيرة (مثل التعليقات) أو أصوات للصورة، وبعض الكاميرات تسمح بحشي الصورة بعد التقاطها. قد تكون هذه المعلومات مفيدة (وخاصة كدليل) لكن يتم تجاهلها في بعض الأحيان.

- قد يكون خيار تسجيل التاريخ والوقت مفعلاً.، مع توضع المعلومات على الصورة عندما يتم التقاطها. كما يمكن تحديد التاريخ والوقت من تاريخ إنشاء ملف الصورة (إذا كانت الساعة صحيحة على الكاميرا و لم يتم تغيير التاريخ عن قصد).
- تستخدم الكاميرات الرقمية افتراضياً تنسيقاً تسلسلياً لتسمية ملفات الصور. فإذا لم تتم إعادة تسمية الملفات المخزنة، يمكن من خلالها تحديد عدد الصور المأخوذة إضافة إلى ترتيب التقاط هذه الصور.
- تخزن الكاميرات الرقمية الصور على بطاقات ذاكرة ومضية، ويجب التحقق منها دوماً لأنه قد تخزن هذه البطاقات أشكالاً أخرى من البيانات.

وحدات GPS

تستخدم أجهزة تحديد الموقع الشامل GPS (Global Positioning System) المعلومات من الأقمار الصناعية لتحدد مكانك الجغرافي بدقة. تم استخدامها بالأصل للإبحار من قبل الملاحين، الطيارين، والمسافرين على الأقدام، حالياً تظهر أنظمة الموقع في السيارات، أجهزة PDA، الحواسب المحمولة، والأجهزة الأخرى. (وهي ملائمة أيضاً للجواسيس لتحديد نقاط الاجتماعات السرية وتبادل المعلومات. كان يملك الجاسوس المدان Patrick Regan وحدة GPS من طراز Garmin III عندما تم القبض عليه).

إذا كنت تملك جهاز GPS، فإنه يمكن فحص واسترجاع ملفات التعقب ونقاط الطرق لتزويد المتطفل بمعلومات حول مكانك ووقت تواجدك في هذا المكان. لقد أصبحت رقاقات GPS أصغر، أرخص، وأكثر فعالية في السنوات الماضية، كما سوف تصبح ميزات "إدراك الموقع" أكثر شيوعاً في المنتجات اللاسلكية، الإلكترونية، الذاتية، والنقالة الخاصة بالمستهلك. وفي أي وقت يتم تخزين معلومات الموقع أو نقلها فهي معرضة لأحد ما يملك الوصول الفيزيائي للوحدة أو يستطيع التنصت على الإرسال.

أساليب: وحدات GPS تلاحقك

لم تستطع Connie Adams، وهي مقيمة في Kenosha، Wisconsin أن تفهم ما الذي يجري. حيث إلى أي مكان كانت تذهب إليه كان يظهر لها رفيقها السابق. حيث كانت تنظر إلى المرآة الخلفية وتراه يلاحقها إلى العمل أو عندما تقوم ببعض المهام. وفي أحد المرات ظهر بشكل مفاجئ في أحد الحانات التي لم تزرها مسبقاً بينما كانت في موعد.

عندما قامت الشرطة بالتحقيقات، اكتشفت أن رفيق Adams السابق Paul Seidler قام بتثبيت جهاز تعقب GPS في سيارتها. وكان الجهاز يبث عن بعد موقعها إلى Seidler، والذي تمكن من مراقبة تحركاتها. وقد أنكر Seidler، في كانون الثاني (يناير) عام 2003، التهم الجنائية الموجهة إليه وهي الملاحقة، السطو، تعريض السلامة للخطر بشكل متهور، والسلوك المخل بالنظام الذي تطبق عليه العقوبة.

استخدم Seidler نظاماً تجارياً من شركة تدعى L.A.S Systems (www.landairsea.com). حيث يبث الجهاز المكلف 695 دولاراً أمريكياً موقع المركبة من خلال شبكة الهواتف الخلوية. حيث تستطيع مشاهدة تحرك السيارة في الزمن الحقيقي على خريطة تُعرَض على شاشة الحاسب أو يمكن إرسال الموقع إلى هاتفك الخلوي على شكل رسالة SMS. لقد تم استخدام مثل هذه المنتجات والتي تسمى (AVL أو Automatic Vehicle Location) لسنوات طويلة لتعقب آثار الشاحنات والمركبات السريعة بصورة شرعية، لكن انخفاض أسعارها وازدياد توفرها يشجع الجواسيس والمتطفلين على حيازتها.

إذا كنت تعرف ماذا تريد فإن وحدات AVL واضحة نسبياً، لكن إذا كنت ترغب بالحصول على جهاز بالفعل صغير وخفي فقد لا تستطيع أن تجده، وفي أي وقت يمكن أن تأخذ فكرة من الإجراءات المضادة الإلكترونية التي يستخدمها الجيش. وقد نشرت المجلة Phrack (المجلة الإلكترونية للقراصنة والمخربين) مقالة حول كيفية بناء يدوياً جهاز لتشويش أجهزة GPS للتغلب على أجهزة التعقب. تتوفر المعلومات والمخططات على الرابط www.phrack.com/phrack/60/p60-0x0d.txt.

طرفيات تحكم ألعاب الفيديو Video Game Consoles

لقد تطور الجيل الأخير من طرفيات تحكم ألعاب الفيديو، مثل Xbox لشركة Microsoft و PlayStation2 لشركة Sony، منذ أيام الطرفيات Pong و Atari 2600. كما تقدم طرفيات تحكم ألعاب الفيديو الحديثة إضافة إلى الصور والأصوات الحقيقية، الأقراص الصلبة الداخلية والاتصال بالإنترنت. كما تحوي طرفية PlayStation مجموعة أدوات إضافية مؤلفة من لوحة مفاتيح، برمجيات، وقرص صلب والذي يسمح لك بأن تحول طرفية التحكم باللعبة إلى حاسب مكتبي ذو النظام Linux. لكن مع كل هذه الميزات المتطورة والبرمجيات، فقد لا تكون طرفية التحكم للهو والألعاب فقط وقد تتمكن من تخزين الملفات والبيانات سرياً والتي قد لا تعرف بوجودها هناك. (اتبع الرابط www.securityfocus.com/news/558 لتطالع مقالة مشوقة حول استخدام طرفيات التحكم للتنصت الحاسبي).

مسجلات MP3 (MP3 Players)

تماماً مثل طرفية التحكم بالألعاب، يمكن أن تكون مسجلة MP3 المحمولة مخزناً سرياً للبيانات. قد تخزن الأحجام الكبيرة من البيانات بالميغا بايت والجيغا بايت، بطاقة ذاكرة ومضية أو قرص صلب داخلي، الموسيقى إضافة إلى أنواعاً أخرى من البيانات. لذلك احذر من أن تفوّت ما يبدو مثل مسجلة راديو أو أقراص مضغوطة عادية. فإذا كان الجهاز يشغّل ملفات MP3 فقد يحوي بيانات أكثر بكثير من مجرد ملفات صوتية مضغوطة.

مسجلات التلفاز الرقمية Television Digital Recorders

لقد حوّلت الخدمات والأجهزة الصلبة مثل الجهاز TiVo مشاهدة التلفاز إلى متعة حقيقية، وذلك عن طريق تسجيل ساعات من برامجك المفضلة رقمياً إلى القرص الصلب. يمكنك تسجيل البرامج التي تختارها دون أن تقلق حول الأشرطة والمؤقتات (إضافة إلى تجاوز الإعلانات في لحظة). يستخدم مسجل الفيديو الرقمي TiVo نظام التشغيل Linux، ومن الممكن تنفيذ جميع أنواع الاختراقات من أجل تحسين الميزات مثل نسخ الملفات من الحاسب إلى جهاز TiVo (اتبع الرابط www.tivofaq.com/hack/faq.html لمعرفة الأسئلة التي تتكرر دوماً). وبما أن جهاز TiVo يبدو مثل جهاز VCR أو جهاز فك التشفير للقمر الصناعي، يمكن لأحد ما يبحث عن دليل رقمي أن يتجاهله ولا يعتبره جهاز تخزين.

تلخيص

الحواسب ليست الأجهزة الوحيدة التي قد يستهدفها الجاسوس لاستخلاص البيانات. فقد يتعرض أي شيء ينقل أو يخزن البيانات للهجوم (وخاصة في التنسيق الرقمي). يمكنك تعزيز أمنك من خلال تنفيذ الخطوات البسيطة التالية:

1. اكتب لائحة بجميع الخدمات أو الأجهزة التي تستخدمها بشكل دوري والتي تقوم إما بنقل أو تخزين المعلومات.

2. ومن ثم، اخفض اللائحة تدريجياً لتتضمن الخدمات أو الأجهزة فقط التي تتعامل مع المعلومات التي تظن بأنها بالغة الأهمية.

3. قم بتحليل اللائحة وقم بمعرفة كيف يتم تخزين أو نقل البيانات، كيف تتم حمايتها، وكيف يستطيع أحد ما الوصول محلياً أو عن بعد إلى المعلومات.

4. بعد أن حددت نقاط الضعف المحتملة، اتبع أساليب جديدة لتقوية البيانات من الهجوم. (تذكر الاختلاف بين المهاجمات الممكنة والمحتملة، وحاول ألا تأخذك مخيلتك إلى البعيد).

التقنيات الجديدة تشق طريقها بشكل متزايد إلى أجهزة الأعمال الإلكترونية (منتجات مثل "عنوانك في كل مكان"، "موقعك معروف"، مزودات تعريف تردد الراديو، منتجات المستهلك المترابطة شبكياً)، كما يزيد احتمال التنصت. فإذا كنت مستخدماً جديداً للتقنيات الحديثة والتي تنقل أو تخزن المعلومات، عليك إدراك أن الميزات الأمنية (في حال كانت موجودة) لن تحل المشاكل الموجودة في إصداراتها الأولى، وقد يكون هناك جاسوس يختبئ في مكان ما ويترقب الفرصة المناسبة لاستغلال نقاط الضعف الجديدة.

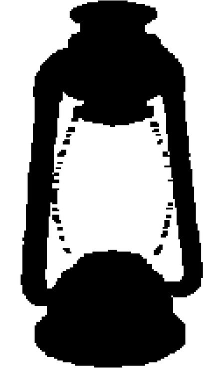


التجسس الحاسبي المتقدم

يبحث هذا الفصل بعض الأساليب المتقدمة والغريبة لإدارة عملية التجسس الحاسبي، والتي تقوم بها عادة الحكومة، الجيش، والجهات المرتبطة بالتجسس الاقتصادي عالي المستوى (بما أن هذه الكينونات تتبع التكتم، فقد تحتاج أحياناً إلى أن تتوقع ما الذي يمكن أن يفعلوه). كما يبحث الفصل أيضاً في بعض التقنيات التي يمكن أن تستخدم في عمليات جمع المعلومات المتطورة والتي لا تتطلب أن تكون أنت وكالة حكومية ممولة جيداً أو وكالة قوى قانون لتتمكن من استخدامها. إذا نظرنا إلى جميع هذه التقنيات من وجهة نظر المستهدَف، فهي تشكل نسبة ضئيلة على لائحة التهديدات التي قد تواجهها، طبعاً ما لم تفعل شيئاً أو تملك شيئاً يجعلك هدفاً لمنظمة جبارة وممولة جيداً.

TEMPEST - التنصت الكهرطيسي

TEMPEST رمز تستخدمه حكومة الولايات المتحدة للإشارة إلى مجموعة معايير سرية للحد من انبثاقات الإشعاع الكهرومغناطيسي من التجهيزات الإلكترونية (تصدر كثير من الأشياء أشعة يمكنها تعريض البيانات للكشف، كما يستخدم الجيش والجواسيس الأشباح مصطلح "أمن الإطلاقات، Emissions Security" أو EMSEC لوصف إجراءات الحماية). تبث الرقاقات المكروية، الشاشات، الطابعات، وجميع الأجهزة الإلكترونية إشعاعاً في الهواء أو من خلال الموصلات مثل الأسلاك أو أنابيب المياه. فعلى سبيل المثال، إذا كنت تستخدم أداة مطبخ أثناء مشاهدة التلفاز، تكون الشحنة الساكنة على شاشة التلفاز هي تداخل سببه الانبثاق من الأداة.



لقد جرت محاولات عديدة لتحويل كلمة TEMPEST إلى اختصار ذو معنى، مثل Transient ElectroMagnetic Pulse Emanation Standard. وتصرح الحكومة رسمياً بأن TEMPEST هي رمز لمجموعة من المعايير، وليس لها أي معنى محدد.

خلال الخمسينيات من القرن الماضي، أصبحت الحكومة قلقة بشأن إمكانية التقاط وإعادة بناء الإشعاعات. من الجلي أن الإشعاعات الصادرة من خلاط كهربائي ليست ذات أهمية، لكن الإشعاعات الصادرة من جهاز تشفير إلكتروني قد تكون كذلك. إذا تم تسجيل الإشعاعات، اعتراضها، ومن ثم إعادة تشغيلها على جهاز مشابه، سوف يكون من السهل جداً كشف محتوى الرسالة المشفرة. كما أظهرت الأبحاث أنه من الممكن التقاط الإشعاعات عن بعد، لذلك بدأ برنامج TEMPEST بالاستجابة.

لقد كان الهدف من البرنامج هو تقديم المعايير التي قد تقلص فرص الإشعاعات الكهرومغناطيسية "المتسربة" من الأجهزة المستعملة لمعالجة، نقل، أو تخزين المعلومات بالغة الأهمية. كما يستخدم المقاولون الحكوميون والوكالات الحكومية حواسب TEMPEST وطرفيات TEMPEST (الطابعات، الماسحات، محركات الأقراص، أجهزة الفأرة، الخ).. لحماية البيانات من التنصت من خلال مراقبة الإشعاعات. يتم تحقيق هذه الحماية نموذجياً بستر الجهاز (أو أحياناً غرفة أو مبنى كامل) بالنحاس أو مواد مُوصِّلة أخرى.

تشكِّل عمليات استشارة برنامج TEMPEST، اختباره، وتصنيعه في الولايات المتحدة عملاً ضخماً جداً، ويقدر بأكثر من مليار دولار أمريكي سنوياً. (ومع ذلك لحق الاقتصاد برنامج TEMPEST أيضاً. إن شراء أجهزة TEMPEST ليس رخيصاً، لذلك تم تنفيذ معيار أقل صرامة للأمن يدعى ZONE. لا تقدم أجهزة ZONE مستوى الحماية الذي تقدمه أجهزة TEMPEST، لكنها أرخص بقليل وتستخدم في الحالات التي لا تكون فيها المعلومات حساسة جداً).

لقد حافظت الولايات المتحدة (وخاصة وكالة الأمن القومي NSA) وحلفاءها بعناد على معايير TEMPEST لكي تظل سرية، لكي لا تستفيد منها الأمم غير الصديقة من أجل ستر أنظمتها الخاصة، نظرياً ليقوم "رجال الخير" بالتجسس عليهم. لكن من جانب آخر، بعد أن أصبح برنامج TEMPEST معروفاً علانية خلال صدوره الأول بصورة غير سرية في عام 1965، تم إفشاء السر، واستطاعت أية قوة أجنبية حتى التي كان لديها تصور بسيط جداً حول التنصت على الإشعاعات استطاعت أن تستخدم سلسلة من الإجراءات المضادة الأساسية ضد هجوم مراقب.

القضية الكبرى المتعلقة بطريقة TEMPEST "الأمن من خلال الغموض" هي أنه استطاعت الوكالات الحكومية والمقاولون الحكوميون (عادة من صناعة الدفاع) الاستفادة من هذه المعايير.

حيث لم تتمكن أية مؤسسة أمريكية بدون امتلاك أمر أمني أن تحمي المعلومات الهامة التي لديها من مهاجمات مراقبة الإشعاعات. إضافة إلى ذلك، كان كل هذا يحصل خلال فترة الحرب الباردة، عندما لم يكن هناك تركيز كبير على التجسس الاقتصادي، لكن بسبب حماية برنامج TEMPEST بشكل كبير جداً، ترك هذا الأمر المؤسسات الكبيرة معرضة للمهاجمات من قبل وكالات الاستخبارات الأجنبية.

بالرغم من أن برنامج TEMPEST كان مكفناً بالسرية والتكتم، لكنه لم يعد كذلك حالياً. حيث يستطيع الشخص الذكي والماهر من خلال التغلغل في مصادر منشورة، ومن ضمنها عدد من المستندات التي نشرت خلال قرار حرية المعلومات Freedom of Information Act، أن يكتشف أحجية برنامج TEMPEST. وبالرغم هذه المعلومات المتوفرة للجمهور، لا يزال هذا المعيار الذي مر على وجوده السري خمسين عاماً تقريباً.

مراقبة الإشعاعات: حقيقة أم خيال؟

إذا كان برنامج TEMPEST يستخدم لمنع أحد ما من اعتراض الإشعاعات، ما هو مدى واقعية تهديد التنصت من خلال مراقبة الإشعاعات؟ إذا كنت قد قرأت من قبل كتاباً حول الأمن الحاسبي أو شاهدت الأفلام أو التلفاز، قد يكون المشهد التالي مألوفاً بالنسبة لك.

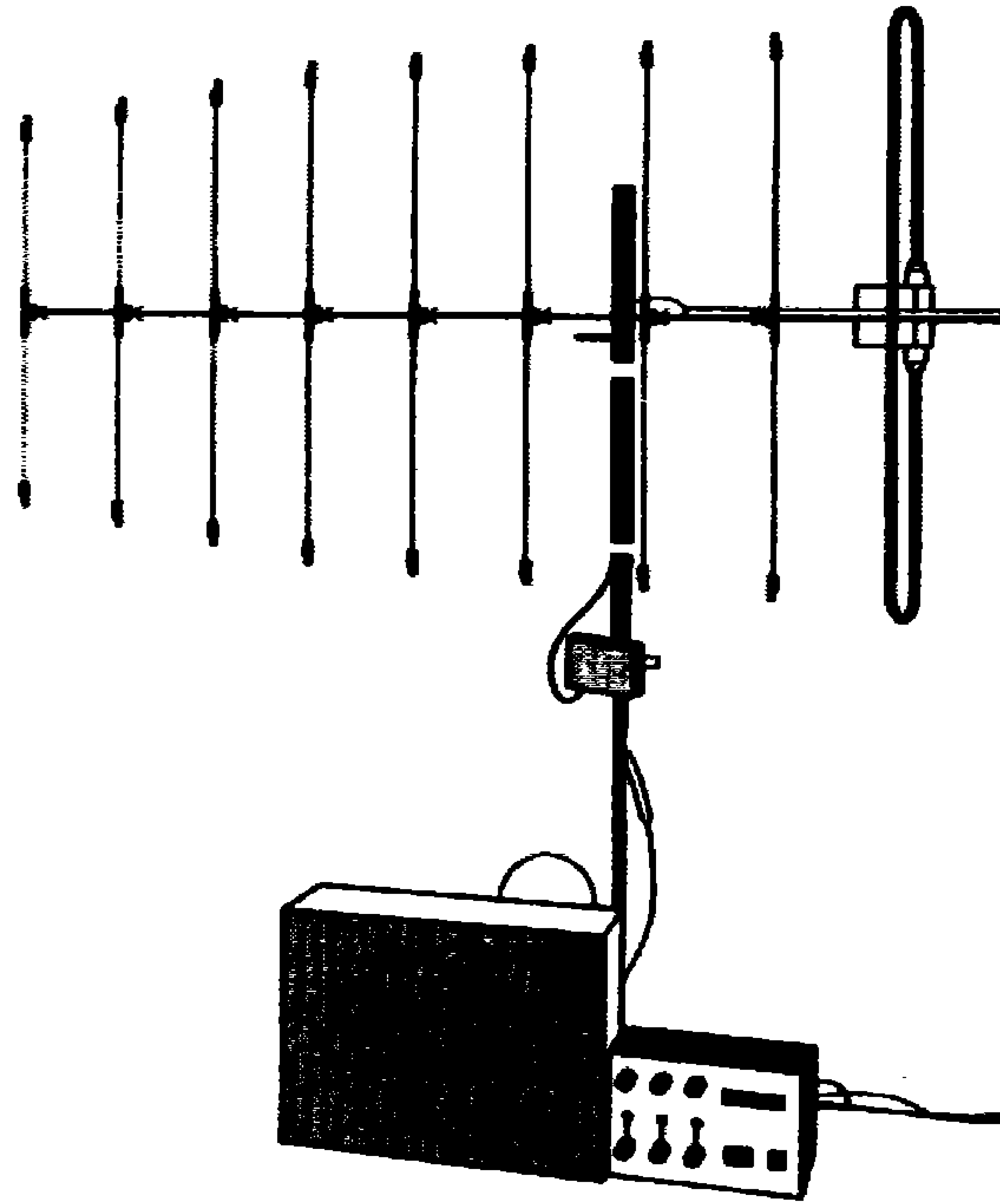
تقف شاحنة دون نوافذ في شارع مظلم. وفي الداخل هوائي موجه عبر لوحة من الزجاج البصري. هدفه هو مكتب في الطابق الثالث. عندما يعمل رئيس الشركة على مستند نصي، ملخصاً استراتيجيته في إدارة خطة معادية لمنافسه، فهولا يعلم أبداً أن كل ما يظهر على شاشته يتم التقاطه، عرضه، وتسجيله في الشاحنة قرب المبنى.

هذا أمر جداً ظريف من وجهة نظر الجاسوس: تنصت سلبي لا يمكن كشفه، لكن قبل أن نناقش فيما إذا كان واقعياً أم لا، يجب أن تتزود ببعض المعلومات. وبما أن معظم الناس لا يملكون أوامر أمنية، تحتاج إلى أن تطلّع على المعلومات المتوفرة للشعب لتنتهي باستنتاجات علمية حول مدى واقعية تهديد مراقبة الإشعاعات.

تاريخ عام مختصر

ظهرت المؤشرات العامة الأولى لإمكانية كون مراقبة الإشعاعات أداة تنصت حيوية خلال منتصف الثمانينيات. حيث نشر Wim van Eck وهو مهندس ألماني في عام 1985 مقالة بعنوان " الإشعاعات الكهرومغناطيسية من وحدات العرض الفيديوية: هل تشكل خطر تنصت؟" شرحت هذه المقالة

كيف يمكنك أن تتنصت على طرفيات العرض الفيديوية (VDTs، Video Display Terminals)، بوادر المراقبات الحاسبية الحديثة من على بعد كيلومتر وباستخدام مكونات رخيصة نسبياً. (لقد كانت المقالة ناقصة عن قصد في عدة نقاط، والتعديلات كانت مطلوبة لبناء جهاز ناجح بالفعل وفق مخططاته. يظهر الشكل 13-1 شكل جهازه).



الشكل (13-1) جهاز مراقبة الإشعاعات الأصلي للمهندس Wim van Eck والذي يستطيع (في الظروف الصحيحة) أن يتنصت على طرفية العرض الفيديوية (VDT) من على بعد كيلومتر واحد.

بعد مرور فترة قصيرة من نشر المقالة، قامت سلسلة من العروض التلفزيونية البريطانية بجعل المراسلين يقودون حول لندن مع أجهزة من نمط جهاز Eck، ويتمتعون بالتنصت على المحامين، المصارف، وشرطة لندن. وبدأ الأشخاص العاملون في الصناعات الأمنية يصبحون متوترين قليلاً حول مشاهد الجواسيس الذين يصلون سرياً إلى بياناتهم حتى من دون أن يطئوا المبنى.

كما باتت وكالة الأمن القومي NSA منفعلة جداً لأن هذه التقنية قد شقت طريقها إلى الشعب. وقد عينت مختبرات الأبحاث Wang (مصنّع ضخم لتجهيزات TEMPEST) موعداً محدداً لاستعراض عمل تجهيزات التنصت للأخصائيين في أمن الحواسب، لكن وكالة الأمن القومي أوقفت العرض

واعتبرته سرياً. كما كانت شركة واشنطن البارزة تتحضر لتقديم عرض في المؤتمر 87 حول "كيف يمكن كشف أمن الحواسب،" مع استعراض تقنيات التنصت باستخدام الإشعاعات، لكن تم إلغاءها في آخر لحظة بطلب من وكالة NSA. (هذا يخالف طريقة الحكومية السويدية المتبعة في الثمانينيات، والتي تضمنت الإعلان عن الأعمال حول التهديد الإجرامي المحتمل للمراقبة بالإشعاعات، كما نشرت كتيباً يسمى "Läckande Datorer" (ارتشاح الحواسب)، والذي وصف هذا التهديد بالتفصيل وتضمن الإجراءات المضادة).

أصبح عدد من المنتجات والمخططات "التابعة لتصميمات van Eck" متوفر تجارياً، في الولايات المتحدة خلال أواخر الثمانينيات، وكثير منها ذو تصميم وفعالية مشكوك بها. استمر وجود هذه المنتجات إلى التسعينيات مع تقديم عدة عروض تلفزيونية لأجهزة المراقبة المفترض بأنها TEMPEST وبيع الأجهزة المزيفة. (يبدو أنه عندما يتعلق الأمر ببرنامج TEMPEST وأجهزة المراقبة تصبح وسائل الإعلام لسبب ما دقيقة الملاحظة لكنها لا تنجز عملها المطلوب).

لقد نتج عن الضجة الإعلامية الكبيرة المحيطة بمراقبة الإشعاعات جميع أنواع المعلومات الخاطئة حول معيار TEMPEST، ومن ضمنها فكرة أنه يستطيع أي شخص صنع جهاز تنصت مع رحلة إلى كوخ الراديو ودفع فاتورة بقيمة 100 دولار أمريكي (ربما يقصدون الجهاز الذي يستطيع اعتراض الإشارات من طرفية عرض فيديوية (VDT) قديمة، لكن بالتأكيد ليس من شاشة حاسب حديث). بالرغم من نشر كثير من المقالات والتي تستعرض التنصت في شروط المختبر، لكن الحقيقة أنه لا توجد أجهزة مراقبة فعالة لتستخدم في مجال التجسس ومتوفرة بسهولة للجمهور.

مع الأخذ بعين الاعتبار الاهتمام الكبير بمعيار TEMPEST وعدد من الأفراد المتميزين ذوي خلفيات إلكترونية وشعبية الإنترنت من أجل نشر المعلومات، إلا أنه لم يقم أحد بنشر مخططات لجهاز مراقبة رخيص وسهل الاستخدام. حيث بالتأكيد مراقبة الإشعاعات ليست عملية سهلة مثل التقاط البيانات اللاسلكية من شبكات 802.11b، كما مر معنا في الفصل الحادي عشر.



يمكن إيجاد تدوين ممتاز لتاريخ الأحداث الرئيسة لمعيار TEMPEST على الرابط http://cryptome.org/tempest-time.htm.

وجهة نظر الحكومة

نعلم الآن أن الشعب لا يشكل تهديداً كبيراً من جانب مراقبة الإشعاعات، لكن ماذا عن الحكومة؟ هنا تبدأ الأمور تصبح غامضة نوعاً ما وذلك بسبب التكتم المحيط بمعيار TEMPEST والحاجة إلى حماية التجسس "المصادر والأساليب."

لا توجد أية سجلات حكومية عامة تعطي فكرة عن كمية المراقبة بالإشعاعات التي تحدث أو حدثت. توجد بعض الحسابات الفريدة المعزولة للمراقبة والتي تم استخدامها للتجسس السياسي، العسكري، والصناعي، ولكن لا توجد معلومات دقيقة تماماً. فعلى سبيل المثال، صرح عميل لمكتب التحقيقات الفدرالي المشارك في فريق MIT عام 1999، أنه يمكن استخدام مراقبة الإشعاعات كتقنية محتملة لإجراء التحقيقات. لكن هل كان تصريحه صحيحاً، مضللاً، أو محاولة مدروسة لتزييف المعلومات؟ لا أحد يعلم.

أحد الصعوبات الأساسية لتعقب حالات مراقبة الإشعاعات هي طبيعتها السلبية وبسبب تنفيذها عن بعد، ومن الصعب اكتشافها ما لم تمسك مرتكب الجريمة بنفسك. لكن حتى لو تم القبض على الجاسوس، فعلى الأغلب لن يتم نشر هذا الحدث، وخاصة إذا كان تجسساً اقتصادياً. تتميز الحكومة والصناعات الخاصة بإخفائها الاختراقات الأمنية عن العامة.

هناك عدد من النقاط التي يمكن أن تجعلنا نعتقد بوجود خطر مراقبة الإشعاعات، على الأقل من قبل خدمات الاستخبارات الأجنبية. حيث أن صناعة تجهيزات TEMPEST تشكل عملاً بأكثر من مليار دولار أمريكي سنوياً، وهذا الأمر يشير إلى وجود تهديد حقيقي لتبرير الحاجة إلى جميع هذه الأجهزة الواقية (أو يمكن أن تكون حيلة كبيرة من أجل جني الأموال الطائلة لعدد قليل من الأشخاص).

كما توجد جميع أنواع المراجع الحكومية والعسكرية لهذا التهديد مثل هذا الاقتباس من كتيب البحرية والذي يتحدث عن "كشف الإشعاعات": "ترتبط الحكومات الأجنبية بشكل مستمر في المهاجمات ضد وحدات معالجة المعلومات والاتصالات الأمريكية الآمنة بهدف وحيد وهو استغلال المهندسين."

إذاً في حال كان التهديد موجوداً، ما هي درجة واقعيته؟ حيث تم رسم صورة مصغرة للتهديد في التسعينيات من قبل سلسلة من التوجيهات الرسمية والتقارير العسكرية والوكالات الحكومية، ومن ضمنها النقاط التالية:

- في عام 1991، دعا تقرير رئيس المفتشين في وكالة الاستخبارات المركزية CIA إلى مراجعة المجتمع الاستخباراتي لمتطلبات أجهزة TEMPEST المترلية والمؤسسة على التهديد المحتمل. اقترحت الحصيلة الناتجة أنه يتم إنفاق مئات الملايين من الدولارات لحماية نقطة ضعف تتمتع باحتمال استغلال ضئيل جداً. وقد أثار هذا التقرير المجتمع الاستخباراتي لمراجعة وتقليص متطلبات أجهزة TEMPEST المترلية.

- في عام 1992، تخلص مكتب الاستطلاع الوطني NRO (National Reconnaissance Office) ووكالة سرية بقيادة الأقمار الصناعية للولايات المتحدة من الحاجة إلى متطلبات أجهزة TEMPEST المترلية.
- في عام 1994، أصدرت الهيئة الأمنية المشتركة تقريراً بعنوان "إعادة تعريف الأمن" إلى وزير الدفاع ومدير الاستخبارات المركزية. وقد أدركت الهيئة الحاجة إلى برنامج TEMPEST واقع عبر البحار، لكنها آمنت بأن احتمال وجود التهديد المترلي هو احتمال ضئيل، واقترحت أن يتم استخدام الإجراءات المضادة لمعيار TEMPEST مترلياً فقط استجابة لبيانات تهديد محددة.

ربما بالغت وكالات الاستخبارات والجيش في تقدير احتمال استغلال نقطة الضعف المتمثلة في مراقبة الإشعاعات بعد اكتشافها في حمية الحرب الباردة الحكومية. لكن بعد أن باشرت متطلبات معيار TEMPEST بالتقدم، أصبح من الصعب جداً إيقافها.

الاستنتاجات

والآن، هل تشكل مراقبة الإشعاعات تهديداً أمنياً حقيقياً؟ بناءً على المعلومات التي عرضناها، يمكن أن نتوصل إلى مجموعة من الاستنتاجات:

- لقد كانت أبحاث van Eck ناجحة في اعتراض الإشعاعات من طرفيات العرض الفيديوية (VDT) البدائية. لكن القدرة على إعادة بناء محتويات شاشة حاسبية متطورة وحديثة عن بعد هو تحدي أكبر بكثير، وخاصة مع وجود أجهزة إلكترونية أكثر والتي تولّد الإشعاعات الكهرومغناطيسية والتي قد تتداخل مع القفل الموجود على الشاشة المستهدفة.
- لا تعتقد الحكومة بأن مراقبة الإشعاعات تهديد كبير للقوى الأجنبية ضمن الولايات المتحدة. لكن الأمور تختلف خارج أراضي الولايات المتحدة مثلاً ضمن سفارة أمريكية أو تنظيم عسكري أمريكي، لأن القوى الأجنبية تكون على أراضيها.
- ليست مراقبة الإشعاعات طريقة تجسسية للعروض التلفزيونية، فهي تشكل تحدياً أكبر بكثير مما قد يعتقد البعض. ما لم يكن خصمك ممولاً جيداً ويملك الوصول إلى التجهيزات الإلكترونية المتطورة والطاقم المدرب ليتمكن من تشغيلها، لذلك ينخفض خطر تهديد مراقبة الإشعاعات بالنسبة لك.

الإجراءات المضادة لأمن الإطلاقات

عندما تختبر أي نوع من الهجوم، تحتاج فعلياً إلى تقدير التكاليف والفوائد من تنفيذه إلى جانب الحماية منه. من وجهة نظر خصمك هل من الأرخص والأكثر فعالية أن يتنكر الجاسوس كحارس

للحصول على المعلومات أو شن هجوم مراقبة متطور وتقني للحصول على نفس البيانات؟ وبالرغم من أنه قد تبرر بعض الأهداف "الصعبة" استخدام طريقة هجوم تقنية مثل مراقبة الإشعاعات، لكن دون شك سوف يتم استخدام طريقة جمع المعلومات البشرية العادية بصورة أكبر.

بما أنه توجد وسائل أرخص وأكثر فعالية لكشف البيانات، لا يحتاج معظم الناس للقلق حول مهاجمات مراقبة الإشعاعات. لكن إذا كان لديك سبب للقلق حول هذا التهديد ولا تملك أمراً أمنياً، يمكنك تطبيق عدد من الإجراءات المضادة، ومن ضمنها ما يلي:

- **شراء تجهيزات TEMPEST المصدقة**: هذا هو الخيار المنطقي إذا كنت وكالة حكومية أو مقاول دفاع. لكن من جهة ثانية فإن الحواسب والطرفيات المصدقة من قبل معيار TEMPEST ليست رخيصة، ولن يبيع معظم البائعين هذه التجهيزات للعامة. لكن تأتي تجهيزات TEMPEST الفائضة إلى الأسواق وغالباً لا تكون مكلفة كثيراً.
- **استخدام تصميم معماري**: البديل الأكثر تكلفة من أجل ستر جهاز وحيد هو ستر الغرفة أو كامل المبنى بشبكة نحاسية ونوافذ خاصة تمنع صدور الإشعاعات. تحقق من المستند العسكري بعنوان "هندسة وتصميم النبضات الكهرومغناطيسية وحماية التسهيلات باستخدام معيار TEMPEST، Engineering and Design – Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities" على الرابط www.usace.army.mil/inet/usace-docs/eng-pamphlets/ep1110-3-2/toc.htm.
- **استخدام تقنيات ستر تردد الراديو النظامي والتداخل الكهرطيسي**: يقدم الوصف الذي عرضه Grady Ward لوسائل الستر بعض الحلول الرخيصة والتي يمكن أن تنفذها بنفسك، مع أن المقالة قديمة قليلاً إلا أنه يمكنك الاطلاع عليها على الرابط www.eff.org/Privacy/Security/tempest_monitoring.article.
- **استخدام خطوط خاصة**: اكتشف كل من Ross Anderson و Markus Kuhn أنه من الممكن التغلب على مراقبة الإشعاعات باستخدام خطوط مصممة بشكل خاص. تتوفر هذه المقالة على الرابط www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf. تدمج الشركة الألمانية Steganos GMbH (www.steganos.com) الخطوط المضادة في بعض منتجاتها، ومن ضمنها تطبيق مجاني لنظام التشغيل Windows من نوع المفكرة.



لمزيد من المعلومات حول برنامج TEMPEST التي تم جمعها خلال السنوات الستة الماضية، اطلع على مقالة Joel McNamara الشاملة بعنوان "المعلومات غير الرسمية الكاملة حول برنامج TEMPEST، Complete, Unofficial TEMPEST Information"، على الرابط www.eskimo.com/~joelm/tempest.html.

معيار TEMPEST البصري - الديودات الضوئية والضوء المنعكس

نشر Joe Loughry في شهر آذار (مارس) عام 2002 مقالة فاتنة حول ما سماه "برنامج TEMPEST الضوئي، Optical TEMPEST". اقتباس من مقدمة المقالة، "لقد تم اكتشاف الشكل غير المعروف سابقاً لكشف الإشعاعات. وقد تم إظهار مؤشرات حالة الديود الضوئي على تجهيزات اتصالات البيانات، تحت شروط معينة، بأنها تحمل إشارة ضوئية معدلة والمرتبطة بشكل كبير بالمعلومات التي يعالجها الجهاز. ليست هناك حاجة إلى الوصول الفيزيائي، حيث يكتسب المهاجم الوصول إلى جميع البيانات المارة عبر الجهاز، ومن ضمنها النص الصريح في حالة أنظمة تشفير البيانات. تظهر التجارب أنه يمكن اعتراض البيانات وفق شروط واقعية من على بعد كبير. كما أن أنواع كثيرة من الأجهزة ومن ضمنها أجهزة المودم وموجّهات بروتوكول الإنترنت معرّضة للمهاجمات."

في وقت لاحق من نفس اليوم نشر Markus Kuhn مقالة بعنوان "مخاطر التنصت البصري في المجال الزمني لشاشات أنبوب الأشعة المهبطية CRT، Optical Time-Domain Eavesdropping Risks of CRT Displays." جوهرياً، يمكن عرض محتويات شاشة الحاسب من خلال الضوء الذي تعكسه على الجدار. وقد صرح Kuhn في الختام، "يمكن إعادة بناء المعلومات التي تعرضها شاشة الحاسب الحديثة ذات أنبوب الأشعة المهبطية من قبل المتنصت من خلال ضوءها المشوش وحتى المنعكس بجميع الاتجاهات، مستخدماً مكونات متوفرة بسهولة مثل أنبوب مضاعفة الضوء حاسب ذو محول سريع من تشابهي إلى رقمي."

هل كانت الحكومة تعلم حول نقاط الضعف هذه سابقاً؟ لا أحد يعلم. وفي كلتا الحالتين، يتطلب الهجوم بعض التجهيزات المتطورة ويمكن التغلب عليها بسهولة ودون تكلفة وذلك بوضع شريط كهربائي أسود فوق أي ديود ضوئي مشع، وبساطة إغلاق الستائر عند التعامل مع المعلومات المهمة (ممارسة جيدة في أي حال).



لمزيد من المعلومات حول هذين النوعين من الهجوم، يمكنك تحميل مقالة Loughry من الرابط http://applied-math.org/optical_tempest.pdf. وتتوفر مقالة Kuhn على الرابط www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf.

المعيار HIJACK والمعيار NONSTOP

هناك معياران سريان مرتبطان إلى حد ما بالمعيار TEMPEST ومرمزان بالأسماء HIJACK و NONSTOP. يشير المعياران HIJACK و NONSTOP إلى كشف الأجهزة المشفرة من خلال

أجهزة إرسال واستقبال الراديو القريبة (مثل الهواتف الخلوية، الراديو المحمول، أو جهاز الاتصال المنزلي intercom). لا توجد كثير من المعلومات، في هذا الوقت، المتوفرة للعامة حول هذين المعيارين وهما أكثر سرية بكثير من المعيار TEMPEST. لكننا إذا حاولنا تجميع المعلومات غير السرية مع بعضها، يمكننا أن نتوصل إلى ما تشير إليه هاتان الكلمتان السريتان.

يرتبط المعيار HIJACK بأحد أشكال كشف الإشعاعات المتعلقة بالإشارات الرقمية مقابل الإشارات الكهرومغناطيسية. كما يشابه هجوم كشف المعلومات بطبيعته الهجوم ضد التجهيزات الصلبة غير المحمية بأجهزة TEMPEST، وحيث لا يحتاج الجاسوس أن يكون قرب الجهاز الذي يتم التنصت عليه. يتطلب الهجوم الوصول إلى خطوط الاتصال (وقد تكون سلكية أو لاسلكية). كما يستخدم الجاسوس الهوائيات، المستقبلات، جهاز عرض، جهاز تسجيل، وجهاز إضافي آخر (وهو نظام كشف خاص والمفترض بأنه حساس جداً، مكلف جداً، ونادر جداً). إلى جانب ذلك، يتطلب التقني الذي يعمل على تشغيل هذا الجهاز كمية كبيرة من الخبرة والممارسة.

أما المعيار NONSTOP فمن الواضح أنه يرتبط بكشف الإشعاعات، لكن يتضمن الإشارات المرسلة من أجهزة تردد الراديو (أجهزة الراديو المحمولة، الهواتف الخلوية، أجهزة النداء، أنظمة الإنذار، الهواتف اللاسلكية، أو الشبكات اللاسلكية، ويتم استثناء مستقبلات البث التجارية AM/FM) قرب جهاز يتضمن معلومات آمنة. توجد خطوط محددة إما لإطفاء جهاز RF أو إبقائه على بعد محدد من الجهاز الآمن، مثل الحاسب أو الطابعة.

برنامج ECHELON - المراقبة الشاملة

حتى الآن، تُستخدم جميع وسائل المراقبة التي تحدثنا عنها حتى الآن على الأغلب للهجوم على حاسب فردي أو شبكة، لكن توجد أداة أكثر فعالية بكثير في مستودع الحكومة لتقنيات التنصت واسمها السري ECHELON.

ECHELON هو عبارة عن برنامج حكومي شامل يستطيع اعتراض مختلف أنواع الاتصالات في أي مكان في العالم. ويتم تشغيله بشكل مشترك من قبل الولايات المتحدة، المملكة المتحدة، كندا، أستراليا، ونيوزيلاندا. ومع أن برنامج ECHELON قد بدأ رسمياً في بداية السبعينيات، إلا أن جذوره تعود إلى عام 1948، عندما قام المشاركون الخمسة في هذا البرنامج بتوقيع اتفاقيات للمشاركة بالمعلومات.

لقد تم اقتراح أن برنامج ECHELON قادر على اعتراض ما يصل إلى ثلاثة مليارات اتصال يومياً، ومن ضمنها رسائل البريد الإلكتروني، رسائل الفاكس، نقل ملفات الإنترنت،

الإرسالات بالأقمار الصناعية، الاتصالات الهاتفية، واتصالات أجهزة التلكس. تعتقد بعض المصادر أن البرنامج يستطيع فحص نسبة تسعين بالمائة من حركة المرور عبر الإنترنت. (لقد تم الاعتقاد أن مصطلح ECHELON يشير إلى اعتراض الاتصالات بالأقمار الصناعية فقط، لكن يشار إليه إلى نظام الاعتراض ككل).

لقد ظل برنامج ECHELON سراً محمياً كثيراً لسنوات طويلة، كما أن حكومة الولايات المتحدة لا تقوم حتى بالتعليق عنه أو تؤكد وجوده (أحياناً عندما يتعلق الأمر بالبرامج التي يجب أن تكون سرية، تتبع الحكومة مبدأ النعامة "الرأس في الرمل"، باعتقاد منها أن عدم قول أي شيء سيجعل المشكلة تنتهي من تلقاء نفسها، وأحياناً هذا أمن عملي صحيح (OPSEC، Operational Security) وأحياناً أخرى فهو مجرد مزاح). إن كل ما نعرفه عن برنامج ECHELON صادر من قبل الوشاة، رسوم الدخول لحكومات أستراليا ونيوزيلاندا، وتقارير عن نظام المراقبة برعاية الحكومة الأوربية، على الأغلب أن ما نعرفه حول برنامج ECHELON هو جزء صغير فقط من مجال وهدف البرنامج.

تأخذ وكالة الأمن القومي الأمريكية NSA موقع القيادة في جميع نشاطات البرنامج، ويتبعها نظرائها الأجانب، رؤساء الاتصالات الحكومية للمملكة المتحدة GCHQ، مجلس إدارة الإشارات الدفاعية الأسترالية DSD، المؤسسة الأمنية للاتصالات الكندية CSE، والمكتب الأمني للاتصالات الحكومية في نيوزيلاندا GCSB. غالباً تتم مشاركة البيانات المأخوذة من البرنامج اختيارياً مع الحكومات الصديقة.

ليس برنامج ECHELON الوحيد من نوعه (مع أنه حالياً الأكبر والأكثر تطوراً). كما تملك الدول الأخرى مثل الصين، الهند، إسرائيل، فرنسا، ألمانيا، باكستان، وروسيا الموارد والوكالات الاستخباراتية للمحافظة على مشاريع اعتراض الاتصالات الخاصة بها (وخاصة الإنترنت).

مبدأ عمل برنامج ECHELON

يعمل برنامج ECHELON مثل المكنسة الكهربائية الكبيرة ويقوم بشفط جميع أنواع المعلومات آلياً. ومن ثم يقوم بتحليل البيانات مستخدماً سلسلة من تطبيقات الذكاء الصنعي الجبارة المؤتمتة. يتم البحث عن كلمات مفتاحية إما للاعتراضات النصية أو الصوتية. (فعلى سبيل المثال، إذا كان "Kim Jong Il" على لائحة الكلمات المفتاحية، وبالتالي ستتم الإشارة إلى أية اتصالات تتضمن ذكر اسم رئيس كوريا الشمالية، لكي يستطيع المحللون عرض المحتويات). قد تكون الكلمات المفتاحية أسماء، عناوين، أرقام الهواتف، عناوين البريد الإلكتروني، أو حتى عينات صوتية، وفي بعض الأحيان قد يتمكن البرنامج عن قصد مطابقة الأصوات إلى هويات

الأشخاص. ويتم الاعتقاد أنه تسمى الأنظمة الحاسبية التي تقوم بتحليل البيانات التي تم تجميعها بالقاموس DICTIONARY.

من الهام معرفة أن برنامج ECHELON هو جهاز محدد واتحاد لجمع المعلومات أيضاً. تملك كل الدول المشاركة في هذا البرنامج أنظمتها وأساليبها الخاصة بها. وتتم مشاركة المعلومات التي تم جمعها بين أعضاء برنامج ECHELON، كما تملك كل وكالة استخباراتية نسخة من قوائم كلمات البحث للوكالات الأخرى. فعلى سبيل المثال، بينما يتم تلقائياً مسح الاتصالات المعترضة، إذا واجهت محطة المراقبة الأسترالية DSD، كلمات مرتبطة بالبرنامج النووي في كوريا الشمالية والتي كانت ضمن لائحة البحث لوكالة الأمن القومي NSA، سوف يتم إرسال البيانات آلياً إلى وكالة NSA عبر شبكة آمنة.

يتم تجميع بيانات الاتصالات بعدد من الطرق المختلفة. حيث يملك النظام سلسلة من الهوائيات الضخمة الموجودة في جميع أنحاء العالم، من أجل اعتراض اتصالات الأقمار الصناعية التجارية. كما يملك البرنامج أيضاً، إضافة لاعتراض إرسالات الأقمار الصناعية، أقماره الصناعية الاستخباراتية الخاصة في مدار الكرة الأرضية مصممة لاعتراض الاتصالات اللاسلكية من المدن الرئيسة إلى الأرض. ومن ثم تنقل أقمار الجواسيس الصناعية البيانات التي تم جمعها إلى مراكز المعالجة في الولايات المتحدة، بريطانيا العظمى، أستراليا، وألمانيا.

أما بالنسبة للاتصالات السطحية مثل الاتصالات الهاتفية ورسائل الفاكس، فقد يملك عضو برنامج ECHELON اتفاقية سرية مع شركة الاتصالات بالتلغراف أو التلفون من أجل توجيه الاتصالات عبر جهاز مراقبة متطور عالي السرعة. ومن المعروف أيضاً نجاح المشاريع المشتركة بين الجيش ووكالات الاستخبارات في التنصت على أسلاك الاتصالات تحت الماء.

لكن بما أن كتابنا يتحدث عن التجسس الحاسبي، سوف نعود إلى القسم حيث يتم فحص نسبة تسعين بالمائة من حركة المرور عبر الإنترنت. وقد صرح Wayne Madsen، صحفي مخابراتي وموظف سابق لوكالة الأمن القومي NSA، في المستند الأوروبي بعنوان "إمكانيات الاعتراض 2000، Interception Capabilities 2000" (www.nrc.nl/W2/Lab/Echelon/ic2kreport.htm)، "قامت وكالة الأمن القومي NSA بتثبيت برمجيات لجمع حركة المرور في تسع نقاط رئيسة لتبادل الإنترنت منذ عام 1995"، (انظر الجدول 1-13) حيث أن نقطة تبادل الإنترنت هي البنية التحتية للشبكة الفيزيائية والغرض منها تسهيل تبادل حركة مرور الإنترنت بين مزودات خدمة الإنترنت. فإذا كنت تراقب جميع نقاط التبادل، تستطيع مراقبة جميع حركة المرور على شبكة الإنترنت. (للحصول على قائمة حديثة بنقاط تبادل الإنترنت، اتبع الرابط www.ep.net/ep-main.html).

الجدول (13-1) نقاط تبادل الإنترنت المزعومة من قبل وكالة الأمن القومي الأمريكية NSA (1995)

موقع الإنترنت	الموقع الجغرافي	العامل	اللقب
FIX East	College Park، Maryland	U.S. Goverment	Federal Information Exchange
FIX West	Mountain View، California	U.S. Goverment	Federal Information Exchange
MAE East	Washington، D.C.	MCI	Metropolitan Area Ethernet
New York NAP	Pennsauken، New Jersey	Sprintlink	
SWAB	Washington، D.C.	PSInet/Bell Atlantic	SMDS Washington Area Bypass
	Chicago، Illinois	Ameritech/Bellcorp	Network Access Point
Chicago NAP	San Francisco، California	Pacific Bell	Network Access Point
San Francisco NAP	San Jose، California	MCI	Metropolitan Area Ethernet
MAE West	Santa Clara، California	CIX	Commercial Internet Exchange

لقد شك مستخدمو الإنترنت المرتابين لوقت طويل أن شبكة الإنترنت مراقَبة. وبالعودة إلى الثمانينيات، ضمّن بعض الأشخاص كلمات مثل NSA، CIA، KGB، plutonium، و Mossad في نهاية رسائل إلكترونية بريئة ورسائل المجموعة الإخبارية USENET كطعم للجواسيس. وقد وصلت هذه الممارسة نصف الجدية نصف الهزلية إلى أوج جديد في الواحد والعشرين من شهر تشرين الأول (أكتوبر) عام 1999 مع ما يسمى "يوم تشويش ECHELON ، Jam Echelon Day" وهو عبارة عن محاولة منظمة لجعل العدد الأكبر من الأشخاص يقومون بتشفير اتصالاتهم بشبكة الإنترنت وتضمين كلمات قادحة في رسائلهم الإلكترونية. وكان الهدف مقصوداً وهو غمر برنامج ECHELON بالبيانات ليصل إلى حالة التوقف التام. بالرغم من أن نجاح هذه المحاولة

مشكوك بأمره، لكن مع ذلك تم تكرار هذا الأمر عام 2001، وعلى الأقل ازداد الإدراك العام لنظام المراقبة هذا.

كما يلاحق برنامج ECHELON بيانات الإنترنت بنشاط بدلاً من التنصت عليها سلبياً. حيث زار التطبيق bot (تطبيق رجل آلي مصمم لجمع المعلومات آلياً من موقع ويب) موقع John Young (cryptome.org) يومياً، محمّلاً أية مواد تم تحديثها. لم يكن تطبيق bot خفياً مع سهولة تحديد عنوان IP له وهو وكالة الأمن القومي NSA وقد كان من الواضح أن هذا التطبيق يجمع المعلومات لصالح برنامج ECHELON.

الخلاف حول برنامج ECHELON والإجراءات المضادة التي يمكن تطبيقها ضده

مع عدم وجود المصادر العديدة التي تؤيد وجود برنامج ECHELON، فقد تعتقد أنه منتج وهمي لإرهابي مستحوذ بنظرية المؤامرة. لكن ليس في هذه الحال، حيث يقلق كثير من الأشخاص حول سرية وطاقة برنامج مراقبة مثل ECHELON، مع أنه يساعد في تعقب آثار المجرمين والتزود بالأدلة لوجود أسلحة الدمار الشامل التي تملكها الولايات المتشردة. من بعض المسائل الأساسية التي تبث القلق في نفوس مؤيدي الخصوصية والبلدان غير المشاركة في نادي ECHELON ما يلي:

- مع أنه تم تطوير برنامج ECHELON بالأصل للتنصت على الاتصالات السياسية والعسكرية خلال الحرب الباردة، لكن وردت تقارير بأنه يستخدم حالياً للتجسس الاقتصادي. وتوجد عدة حالات حين قامت المؤسسات الأمريكية بهزيمة منافسيها الأوروبيين عن قصد في عقود مربحة مبنية على بيانات برنامج ECHELON.

- تملك حكومة الولايات المتحدة وحكومات بلاد أخرى قوانين خصوصية محلية تمنع وكالات الاستخبارات الأجنبية من أن تتجسس على مواطنيها. لكن توجد شكوك بأنه تم استخدام برنامج ECHELON لتجاوز هذه القيود. فعلى سبيل المثال، بالرغم من أن وكالة الأمن القومي NSA لا تستطيع التجسس قانونياً على مواطن أمريكي إذا امتلك رؤساء الاتصالات الحكومية للمملكة المتحدة GCHQ بيانات من برنامج ECHELON مرتبطة بهذا الفرد، لكنها تستطيع تمرير المعلومات إلى نظرائها في وكالة NSA المهتمين بالموضوع.

- لا توجد أية تدقيقات، موازنات، أو مراقبة لوقف الاختراقات ضمن برنامج ECHELON. حيث صرحت جريدة Washington Post في كانون الأول عام 1998 أن وكالة الأمن القومي NSA قد اعترفت بأنه لديها معلومات عن الأميرة ديانا أميرة Wales وبعضها يعتمد

على مكالمات هاتفية تم اعتراضها. و لم يتم إعطاء أي تفسير عن امتلاك وكالة استخبارات أمريكية معلومات عن فرد سابق للعائلة الملكية البريطانية.

لن ندخل في المجادلة حول "ليس لدي أي شيء أخفيه، لذلك لا داعي للقلق حول برنامج ECHELON " لنفترض بأنك مؤيد الخصوصية الشخصية أو لديك شيء ما لتخفيه. إن قيامك بتحميل ملفات MP3 لن يثير اهتمام برنامج ECHELON ولن يقوم بمراقبة هواياتك بتسجيل الأغاني (لكن قد ترغب بذلك الجمعية الأمريكية الصناعية للتسجيل). حيث يجمع ويلاحق برنامج ECHELON الكثير من البيانات، وما لم تقم بأمر شرير جداً سوف تضيع ضمن الحشود.

كما يجب أن تعلم أن برنامج ECHELON هو ببساطة تقنية للمراقبة، ومع أنها تقنية متطورة وجبارة، ويمكن التغلب عليها مثل أية طريقة تنصت أخرى. بعض الإجراءات المضادة التي يمكن استخدامها ضد برنامج ECHELON ما يلي:

- **التشفير**: من الواضح جداً أنك إذا قمت بتشفير البيانات التي ترسلها عبر الإنترنت باستخدام خوارزمية تشفير قوية، سوف يكون من الصعب جداً لأحد ما أن يكشف المعلومات. لكن قد يلتقط برنامج ECHELON الاتصالات المشفرة التي يعترضها لمجرد كونها مشفرة (أحد ما يملك شيئاً ما ليخفيه). وإذا انتهى بك الأمر كهدف حكومي، سوف تحصل محاولات عديدة لاختراق التشفير. وإذا لم يتم فك تشفيرها، فعلى الأغلب سوف يتم تخزينها مع ملايين الرسائل السرية الأخرى لتخضع إلى تحليل الشيفرة المحتملة في لحظة ما في المستقبل (باستخدام اختراق عاملي، حاسب كمي، تقنية غريبة، أو أي شيء آخر).
- **القنوات السرية**: بدلاً من أن تستخدم التشفير الذي يمكن أن يلفت انتباه إليك، تستطيع استخدام قناة سرية لإخفاء اتصالاتك، والتي يمكن أن تكون إخفاء رسالة بصيغة رسالة لا طائل منها أو تضمين رسالة ضمن صفحة ويب. نصح المتهم Patrick Regan العراقيين أن يغيروا موقع الويب الخاص بالأمم المتحدة ليشير فيما إذا كانوا مهتمين في شراء الأسرار العسكرية والاستخباراتية منه.
- **تقنية غير متطورة**: إذا كنت مرتاباً بالفعل من برنامج ECHELON ولديك شيء ما تخفيه، يمكنك دوماً اللجوء إلى وسائل الاتصالات القديمة والتي لا تستخدم الحواسب، الهواتف، أو أجهزة الراديو. بعد أن تفهم أعضاء تنظيم القاعدة إمكانيات المراقبة لدى الولايات المتحدة خلال اجتياح أفغانستان، توقفوا عن استخدام هواتف الأقمار الصناعية وأجهزة الراديو وبدؤوا يعتمدون على الرسل من أجل تمرير الرسائل.

أساليب: الولايات المتحدة ضد Regan

عمل Brian Patrick Regan لصالح مكتب الاستطلاع الوطني NRO، وهو الوكالة المسؤولة عن الأقمار الصناعية الأمريكية المراقبة. عمل في بداية الأمر لصالح المكتب NRO بصفته رقيب أول في القوى الجوية حيث كان يطلّع على الأمور السرية للغاية وحتى المعلومات الأكثر أهمية. وعندما تقاعد Regan من الجيش عام 2000، استمر العمل مع مكتب NRO بصفته مقاولاً لشركة TRW المتحدة، والتي تم اكتسابها لاحقاً من قبل شركة Northrop Grumman.

تم اعتقال Regan في الثالث والعشرين من آب (أغسطس) بتهم محاولته بيع معلومات سرية، ومن ضمنها صور الأقمار الصناعية، إلى العراق، ليبيا، والصين. عندما تم إيقافه في المطار العالمي Dulles قبل أن يصعد على متن الطائرة المتوجهة إلى Zurich، وجد عملاء مكتب التحقيقات الفدرالي بأنه كان يحمل إحداثيات مشفرة لمواقع القذائف إلى العراق والصين، حيث لم تكن المعلومات حول أنواع القذائف وتواريخ القذائف واضحة في بداية الأمر، وقد أتت المعلومات من صور الأقمار الصناعية التجسسية الأمريكية.

وقد قام مكتب التحقيقات الفدرالي باسترداد رسائل موجهة إلى العراق وليبيا من حاسبه المحمول المأخوذ من منزله. وقد عرض Regan على هذين البلدين بأن يزودهما بالمعلومات السرية مقابل 13 مليون دولار أمريكي. وقد بدأت جميع الرسائل بالعبارة، "أنا مستعد أن أرتكب التجسس ضد الولايات المتحدة."

لقد كان Regan قلقاً حول مكافحة المراقبة من قبل مكتب التحقيقات الفدرالي (كان يجب أن يقلق لأن مكتب التحقيقات الفدرالي كان يتبعه إلى مكتبة عامة ويراقبه وهو يتصفح الويب بحثاً عن العناوين وأرقام الهواتف للسفارات الأجنبية)، لذلك قرر أن يستخدم قناة سرية كجزء من اتصالاته مع العراقيين.

لقد تم تضمين نسخة من رسالة Regan إلى الرئيس صدام حسين، في تهمته. وفيما يلي جزء من هذه الرسالة (لم يتم تغيير الأخطاء المطبعية والقواعدية)، "الشيء الأول الذي أريدك أن تقوم به هو تغيير بسيط جداً في صفحة الأمم المتحدة الخاصة بك على الويب لكي تثبت لي أنك لست فخاً من قبل مكتب التحقيقات الفدرالي. لقد طبعت الصفحة المطلوبة ... فإذا قمت ببعض التغييرات البسيطة لهذه الصفحة (تبديل كلمة بأخرى، إضافة فاصلة، أو تغيير بعض الأرقام) هذا سيثبت بأنك تلقيت كلتا الرسالتين وتخطط للاستمرار بالخطة." وتقريباً تم إرسال نسخة مشابهة لهذه الرسالة إلى الرئيس الليبي معمر القذافي.

بدأت محاكمة Regan في بداية عام 2003. ولقد كانت هذه المحاكمة هي المحاكمة التجسسية العلنية الأولى لمواطن أمريكي متهم بالتجسس منذ خمسين سنة. حيث قام كل من الجواسيس المدانين Walker، Pollard، Hanssen، Ames وغيرهم من الجواسيس المعروفين بالاعتراف بجريمتهم أمام الحكومة ولم يمروا بمحاكمة أصلاً. ادعى Regan بأنه لم

يقم بتزويد أية معلومات سرية لقوة أجنبية، وجميع المعلومات التي امتلكها كانت متوفرة للجميع. وقد تمت إدانته وحكم عليه بالسجن المؤبد في شهر آذار (مارس) عام 2003.



لمزيد من المعلومات عن برنامج ECHELON، قم بزيارة موقع ACLU ECHELON، على الرابط www.echelonwatch.org ومجموعة موقع cryptome لمستندات عن برنامج ECHELON، على الرابط http://cryptome.org/cryptout.htm/Echelon.

نظام CARNIVORE/DCS-1000

CARNIVORE (المعروف حالياً باسم DCS-1000، وهو نظام المجموعة الرقمية (Digital Collection System)) وهو نظام حاسبي لمكتب التحقيقات الفدرالي من أجل إدارة عمليات التنصت على اتصالات الإنترنت. على خلاف طريقة برنامج ECHELON في العمل مثل المكنسة الكهربائية، يقوم نظام CARNIVORE بالتنصت على البيانات المرتبطة بفرد مستهدف فقط.

CARNIVORE بالأساس هو حزمة برنامج sniffer متطورة مصممة خصيصاً للاستخدام من قبل قوى القانون. ويتم تثبيتها على مزود خدمة الإنترنت الخاص بالمشتبه به بعد الحصول على أمر من المحكمة. (يؤكد مكتب التحقيقات الفدرالي بأنه يتم استخدام نظام CARNIVORE عندما لا يستجيب مزود خدمة الإنترنت للأمر من المحكمة بحثاً عن معلومات محددة). حيث تمر الأداة الاستخباراتية خلال حركة المرور القادمة والصادرة، مسجلةً البيانات المرتبطة بالهدف وفق أمر بالتنصت من المحكمة. حيث يمكن أن يعمل نظام CARNIVORE إما مثل "متنصت للمحتوى" أو مثل "جهاز تعقب السجلات"، كما يلي:

- **متنصت للمحتوى:** يلتقط كل حركة المرور للبريد الإلكتروني أو الشبكة الموجهة من وإلى عنوان IP محدد أو مستخدم محدد. هناك نموذجياً متطلبات أكثر صرامة من المحكمة لهذا النوع من التنصت.
- **سجل التعقب:** يلتقط معلومات المناقلات فقط، دون محتوى. أمثلة على هذا النوع، ترويسات البريد الإلكتروني (باستثناء موضوع الرسالة) أو مواقع الويب أو ملقمات FTP التي تمت زيارتها. عادة من الأسهل الحصول على أمر لهذا النوع من التعقب مقارنة مع متنصت المحتوى.

ظهر برنامج CARNIVORE للعامة لأول مرة في صيف 2000، وكل ما نعرفه عنه يأتي من حوالي 600 صفحة من مستندات مكتب التحقيقات الفدرالي المنشورة بموجب قرار حرية المعلومات إلى مركز المعلومات السرية الإلكترونية (لقد تم تنقيح كثير من هذه الصفحات بصورة كبيرة) كما تمت إدارة المعلومات المزودة من المراجعة المستقلة لبرنامج CARNIVORE من قبل معهد Illinois للتقنيات.

نظرة عامة لبرنامج CARNIVORE

برنامج CARNIVORE هو جزء من مجموعة الأدوات الاستخباراتية الخاصة بمكتب التحقيقات الفدرالي والمعروفة بالاسم مجموعة DragonWare. إلى جانب برنامج CARNIVORE، يوجد البرنامجان CoolMiner و Packeteer. حيث يقوم برنامج Packeteer بمعالجة الخرج الخام لبرنامج CARNIVORE ويعيد بناء البروتوكولات (مثل بروتوكولات SMTP و HTTP) من حزم IP. أما برنامج CoolMiner فيقوم بإنشاء ملخصات ساكنة وينسق معلومات المحتوى لإظهارها باستخدام مستعرض ويب. (تتألف برامج DragonWare من ملفات الربط الديناميكي DLL مبرمجة بلغة ++C وواجهات مرئية مطورة باستخدام لغة البرمجة Visual Basic).

طوّر مقاول من فريق ثالث برنامج CARNIVORE، كما تم تنقيح جميع المراجع إلى هوية المطوّر لتشير إلى مستندات قرار حرية المعلومات، لكن كانت هناك إشاعات غير مدعومة بأدلة بقيام الشركة Booz، Allen & Hamilton وهي شركة دفاعية ضخمة ولهندسة واستشارة المعلومات بدور كبير في تطوير برنامج CARNIVORE وتطبيقات مراقبة حاسبية أخرى لمكتب التحقيقات الفدرالي.

يؤكد مكتب التحقيقات الفدرالي أنه ليس هناك أي خطأ في اختيار الاسم CARNIVORE للبرنامج (معنى كلمة carnivore: حيوان من آكلات اللحوم). وتوجد آراء متعددة في الموضوع، وتبعاً للشخص الذي تتحدث معه في المكتب، فقد تتلقى إجابات مثل "يحصل النظام على لحم التحقيقات"، أو "يقوم آكل اللحوم بمضغ جميع البيانات على الشبكة، لكنه فعلياً يأكل المعلومات المخولة من قبل أمر من المحكمة." وظل مكتب التحقيقات الفدرالي مصرّاً، عند تغيير اسم البرنامج إلى DCS-1000، أنه لا توجد أية علاقة لهذا التغيير برد الفعل العام السلبي للاسم القديم.

ظهر برنامج Carnivore في عام 1999، لكن كانت هناك على الأقل أداتان للمراقبة قبل ظهوره. حيث كان سابقه برنامج Omnivore (الحيوان آكل كل شيء) وكان يعمل على نظام التشغيل Solaris من شركة Sun. تم تصميم البرنامج لمراقبة الرسائل الإلكترونية الواردة والصادرة، طباعة المحتويات في الزمن الحقيقي، وتخزين البيانات على أشرطة بحجم 8 مم. وقد استبدل برنامج

Omnivore، الذي استخدم لأول مرة عام 1997، أداة قبله والتي لم يتم كشف اسمها، وما يزال البرنامج سرياً.

لم يرغب مكتب التحقيقات الفدرالي بنظام التشغيل Solaris وأراد استخدام شيء أبسط، لذلك بدأ المكتب مشروع تطوير اسمه السري "Phiple Troenix" (توجد نخلة اسمها Phiple Troenix، لكن لا أحد يعلم بماذا كان يفكر المكتب أو المقاول عندما أطلقوا هذه التسمية). تم تصميم برنامج Phiple Troenix، والذي تحول أخيراً إلى برنامج Carnivore، ليعمل على أنظمة التشغيل Microsoft Windows NT. وقد تم تخصيص ميزانية بقيمة 800,000 دولار أمريكي لمشروع نقل برنامج Omnivore إلى منصة تشغيل جديدة والتدريب على استخدامه.

لقد كانت الإصدارات الأولى من برنامج Carnivore مليئة بالأخطاء، مما دعا إلى بدء مشروع "Carnivore المطوّر، Enhanced Carnivore" في عام 1999. وقد تم تصميم الإصدارين 2.0 و 3.0 مع ميزات جديدة، وفقاً لمستندات قرار حرية المعلومات، مثل القدرة على التنصت على اتصالات من خلال الصوت عبر بروتوكول IP.

تم تثبيت برنامج Carnivore على حاسب Pentium III ذو نظام التشغيل Windows NT وبطاقة Ethernet سرعتها 10Mbps/100Mbps ومحرك Iomega Jaz لتخزين البيانات التي تم التقاطها (المحرك له قفل فيزيائي لمنع الوصول غير المخول إليه). تم وصل آلة Carnivore إلى شبكة مزود خدمة الإنترنت مع جهاز تفريغ للتنصت Shomiti. كما تم تثبيت، إضافة إلى نظام التشغيل ونسخة برنامج Carnivore، برنامج pcAnywhere للسماح للعميل أن يتحكم عن بعد بالحاسب عبر خط الهاتف.

لقد كان عميل مدرب تقنياً TTA مسؤولاً عن تثبيت برنامج Carnivore وتكوين البرنامج مع عنوان IP أو عنوان البريد الإلكتروني للمشتبه به (يمكن تطبيق قواعد ترشيح أخرى أيضاً). ومن ثم يقوم برنامج Carnivore بفحص حركة مرور الشبكة، ونسخ الحزم فقط من أو إلى موقع أو هدف محدد. ويتم تجاهل جميع الحزم الأخرى المارة عبر الشبكة.

يتم تخزين كل البيانات على محرك أقراص Jaz سعته 2GB. ومن ثم يقوم العميل باسترجاع القرص بشكل دوري ووضعه ضمن وعاء قديم ومختوم للحفاظ على الدليل (راجع الفصل الخامس). ومن ثم يتم فحص الدليل باستخدام أدوات أخرى من مجموعة DragonWare للتحقق من فعالية الدليل وإمكانية استخدامه ضد المشتبه.

بعد الانتهاء من عملية المراقبة (نموذجياً، تمنح المحاكم فترة أولية بثلاثين يوماً لمهام التنصت)، ومن ثم تتم إزالة الجهاز من شبكة مزود خدمة الإنترنت.

الخلاف حول برنامج Carnivore والإجراءات المضادة التي يمكن تطبيقها ضده

الاهتمام الأكبر الذي أثاره مؤيدو الخصوصية بشأن برنامج Carnivore، هو حقيقة أن النظام يصل ويعالج حركة المرور القادمة والصادرة، ومن ضمنها للمستخدمين غير المستهدفين للمراقبة والذين لم تذكر أسماءهم في أمر المحكمة.

عندما تسربت الإشاعات حول برنامج Carnivore في عام 2000، ظهرت صيحة عالية من قبل الشعب ضد هذه الأداة بناءً على الانتهاكات المحتملة للحريات المدنية. (لقد انزعج مكتب التحقيقات الفدرالي من هذه الضجة الكبيرة حول البرنامج، لأنه كان لديهم عشرين آلة فقط للبرنامج تم استخدامها العام الماضي ما لا يزيد عن 25 مرة).

وبسبب هذا الخلاف، سمح مكتب التحقيقات الفدرالي بإجراء مراجعة مستقلة لبرنامج Carnivore واختار معهد Illinois للأبحاث التقنية ليتولى إدارته. (لم يتقبل مؤيدو الخصوصية هذا الأمر لأنه كان يجب الانتهاء من المراجعة في غضون ستة أسابيع، كما تألف فريق المراجعة من عدد من العاملين لصالح الحكومة ومن ضمنهم أناس من وزارة العدل، وكالة الأمن القومي NSA، ووزارة الدفاع).

لقد أزال الإصدار الأخير من التقرير في شهر كانون الأول عام 2000 الكثير من الغموض التقني المحيط ببرنامج Carnivore، وتضاءل الخلاف حول برنامج Carnivore ببطء. (يمكنك عرض التقرير على الرابط www.cdt.org/security/carnivore/001214carniv_final.pdf). لكن قام برنامج Carnivore بالكشف عن أنيابه مرة أخرى خلال ربيع عام 2002، عندما تم اكتشاف أن برنامج الالتقاط هذا كان يجمع الرسائل الإلكترونية من الأفراد الذين لم يكونوا ضمن أمر التنصت الصادر من المحكمة خلال تحقيق متعلق بالإرهاب. صرحت المذكرات الداخلية لمكتب التحقيقات الفدرالي بأن برنامج Carnivore كان مائلاً ليسبب "التقاط بيانات خاطئ"، مع أخذ الملاحظة بأنه "تستطيع الاعتراضات غير المخولة انتهاك خصوصية المواطنين، إضافة إلى إفساد التحقيقات الجارية بصورة جدية"، وصرحت بأن هذه الاعتراضات غير شرعية.

سوف يستمر مكتب التحقيقات الفدرالي باستخدام برنامج Carnivore في حربه ضد الإرهاب، وربما بدرجة موسعة. وبالرغم من احتمال إصلاح الأخطاء المتعلقة بجمع البيانات غير الصحيحة، لكن هناك احتمال لإساءة الاستخدام. يمكن استخدام جميع الإجراءات المضادة القياسية المستخدمة في أشكال التنصت الأخرى للحد من فعالية برنامج Carnivore. تتضمن هذه الإجراءات استخدام التشفير، استخدام البريد الإلكتروني المجهول، وملقمات الويب المجهولة.

(للقراء الذين يعملون في وكالات قوى القانون، هذه الإجراءات المضادة ليست جديدة أو ثورية ولا يعني ذكرها إعطاء الأشرار طريقة لمخالفة القانون. لكن الحقيقة بأن المجرمون سوف يستخدمون بشكل متزايد عدد من التقنيات لمقاومة جهودك. وبالرغم من أن التشريع يحظر استخدام أدوات خصوصية محددة، لكن هذا لن يمنع الأشخاص الخارجين عن القانون من استخدامها. ويجب أن تدرك هذا عاجلاً، وأن تعرف بأنك قد تحتاج إلى تغيير تقنيات التحقيق التي تستخدمها عند التعامل مع هدف خبير تقنياً).



لمزيد من المعلومات حول برنامج Carnivore، اطّلع على مجموعة الموارد التابعة لمركز المعلومات الإلكترونية السرية، على الرابط www.epic.org/privacy/carnivore/.

الفانوس السحري Magic Lantern

من الواضح أن مكتب التحقيقات الفدرالي يتطلع إلى مستقبل الاتصالات الرقمية ويحاول الحفاظ على تقنيات التحقيق لديه لتتوافق مع التقنيات المتطورة. حيث ظهرت معلومات في نهاية عام 2001 حول مشروع مراقبة آخر لمكتب التحقيقات ويسمى الفانوس السحري Magic Lantern. وفقاً لمصادر من مكتب التحقيقات، فإن مشروع الفانوس السحري لا يزال قيد التطوير (نموذج أولي). ونعلم من الأوصاف السطحية التي حصلنا عليها، بأن الفانوس السحري هو تطبيق حصان طروادة والذي يقوم العميل بتثبيته على حاسب المشتبه به ويقوم بتسجيل ضربات المفاتيح وجمع الأدلة. الاختلاف بين مسجل المفاتيح هذا ومسجل المفاتيح الذي تم استخدامه في قضية Scarfo هو عدم حاجة العملاء إلى الوصول فيزيائياً للحاسب، إنما يمكنهم تثبيت تطبيق حصان طروادة عبر ملف مرفق بالبريد الإلكتروني أو من خلال أحد ثغرات نظام التشغيل Windows.

بدأت تجـول جميع أنـواع الإشاعـات حـول الفـانوس السحـري، ومن بينها أن شركة Codex Data Systems هي المطوّر الأساسي للمشروع، وأن البرنامج مبني على منتج للشركة يسمى Data Interception by Remote Transmission (D.I.R.T).. وقد حاول مدير الشركة Frank Jones أن يبيع البرنامج .D.I.R.T لكثير من الوكالات القانونية. ولسوء الحظ، لم يقم عدد من الوكالات الفدرالية (والحكومات الأجنبية) بالتحقيق الكافي لمعرفة أن Frank Jones هو شرطي مطرود في مدينة نيويورك ومجرم مدان، وذاك لحيازته غير القانونية لأجهزة المراقبة، وله تاريخ طويل في بيع المنتجات الأمنية. (قضى Jones فترة إدانته في السجن وقد كان يسمي نفسه ملك الجواسيس، وكان يدّعي بأنه حالته العقلية هي التي تسببت في قيامه بأمور خارجة عن

القانون، والتي تابع القيام بها بعد خروجه من السجن. وفي عام 2001، تلقى الموظف القضائي المسؤول عن Jones توبيخاً صارماً بسبب إغفاله عدة انتهاكات قام بها Jones). إنه لأمر مشكوك به أن يستخدم مكتب التحقيقات الفدرالي منتج .D.I.R.T، لكن تحصل أمور غريبة دوماً عندما يتعامل مكتب التحقيقات مع المجرمين الخبراء بالتقنيات العالية.

تماماً كما حصل ببرنامج Carnivore خلقت المعلومات المتسربة حول الفانوس السحري جدلاً شعبياً كبيراً. كما صرح ممثلون لشركات مكافحة الفيروسات الشهيرة مثل شركة Symantec (منتجها Norton AntiVirus) وشركة McAfee بأن منتجاتها لن تستطيع كشف حصان طروادة الحكومي (لكنها سحبت هذه التصريحات لاحقاً)، بينما صرّحت شركات مكافحة الفيروسات الأخرى بأنها بالتأكيد سوف تُعلم المستخدمين فيما إذا كان البرنامج الحكومي مثبتاً على أنظمتهم. (لكن الحقيقة أن استخدام برنامج الفانوس السحري نادراً جداً، وبالتالي لن تضع برمجيات مكافحة الفيروسات يدها على نسخة حقيقية من البرنامج لتضيفه إلى قاعدة البيانات الخاصة بالفيروسات وتطبيقات حصان طروادة).

منذ صدور الأخبار الأولية حول مشروع الفانوس السحري، لم تتسرب أية معلومات إضافية حول تطبيق حصان طروادة أو أية مشاريع مراقبة أخرى تابعة لمكتب التحقيقات الفدرالي. مع إمتلاك بعض الأشخاص من خارج الحكومة إمكانية الوصول إلى الفانوس السحري وتطبيقات حصان طروادة أخرى مشابهة، وإضافة إلى استخدام منتج مسح تجاري، فإن معظم الإجراءات المضادة التي مرت معنا في الفصل التاسع يجب أن تثبت فعاليتها في الكشف والتغلب على هذه الأنواع من تطبيقات التنصت.



يتضمن موقع الويب الخاص بـ John Young كمية كبيرة من المعلومات حول منتجات .D.I.R.T و الفانوس السحري Magic Lantern (ومن ضمنها نسخة تنفيذية لبرنامج .D.I.R.T، والتي تم الحصول عليها بطريقة مجهولة). اتبع الرابط http://cryptome.org/dirt-guide.htm، cryptome.org/dirty-lantern.htm و cryptome.org/dirty-secrets2.htm.

تطبيقات ومكونات نظام تشغيل معدّلة

توجد طريقة متطورة أخرى لكشف البيانات بالغة الأهمية وهي استبدال تطبيق أو أحد مكونات نظام التشغيل (مثل مكتبة ما) بإصدار معدّل والذي إما أنه يقوم بتسريب المعلومات أو يجعل المعلومات الآمنة عرضة للهجوم. وقد يقوم البرنامج التنفيذي المعدَّل بنشاطات تجسسية، كما يلي:

- إضعاف برمجيات التشفير (وضع مساوئ أو مفاتيح إضافية للخوارزمية التي تسهّل عملية فك التشفير)
- السماح بنشاطات شبكية غير مخولة (مثل إصدار معدّل من تطبيق جدار حماية والذي يسمح سرياً بإجراء اتصالات محددة)
- تسجيل البيانات سرياً (تسجيل ضربات المفاتيح)

غالباً تسمى البرامج التنفيذية والمكتبات المعدلة بالأبواب الخلفية أو تطبيقات حصان طروادة، لكن يوجد اختلاف هام بين البرامج التنفيذية المعدلة و تطبيقات حصان طروادة التي مرت معنا في الفصل التاسع. حيث تعدّل معظم تطبيقات حصان طروادة البسيطة نظام التشغيل من خلال الذاكرة عن طريق التقاط استدعاءات API في النظام Windows. وهذا يعني تنفيذ شيفرة إضافية قبل أو بعد استدعاء API. التقاط الاستدعاء عملية بسيطة، لكن يجب أن يتم أولاً تنفيذ تطبيق ما لكي يتم تعديل استدعاء API.

تتضمن طريقة متطورة أكثر تعديل نسخة من برنامج تنفيذي قبل البدء بالهجوم ومن ثم التبديل بين البرنامج التنفيذي الأصلي بالإصدار المعدل، إما عن طريق الوصول الفيزيائي إلى الحاسب أو استغلال أحد ثغرات الشبكة.

توجد طريقتان لتعديل التطبيق أو أحد مكونات نظام التشغيل:

- **إعادة ترجمة المصدر**: هذا يتضمن إجراء تغييرات على الشيفرة المصدرية ومن ثم إعادة ترجمة المكتبة أو البرنامج التنفيذي. (حتى لو لم تكن تملك الشيفرة المصدرية الأصلية، لا يزال من الممكن صنع إصدار معدل من الإصدار الأصلي).
- **ترميم البرنامج التنفيذي**: وهذا يتضمن استخدام محرر لتعديل البرنامج التنفيذي وذلك عن طريق تغيير التمثيلات الست عشرية لتعليمات متنوعة للغة assembly. حيث يتم أولاً فحص البرنامج التنفيذي باستخدام المفكك (وهو أداة تحوّل التطبيق إلى لغة assembly التي يمكن قراءتها) وذلك من أجل تحديد التعليمات الواجب تعديلها.

يعتقد بعض الأشخاص أن البرمجيات الامتلاكية مثل نظام التشغيل Windows، حيث يمنع نشر الشيفرة المصدرية، أكثر أماناً من البرمجيات مفتوحة المصدر مثل نظام Linux. ويتم الجدال بسبب عدم إمكانية الوصول إلى الشيفرة المصدرية، وبالتالي لا تستطيع أن تضيف شيفرة خبيثة ومن ثم إعادة الترجمة ونشر البرنامج التنفيذي أو المكتبة إلى الضحية.

بالرغم من أن امتلاك الشيفرة المصدرية يسهّل كثيراً تعديل نظام التشغيل أو التطبيق لأغراض تجسسية، لكن عدم امتلاكها لن يوقف خصماً خبيراً ومصمماً. حيث كل ما يتطلب الأمر هو معرفة لغة assembly، مفكك، ومترجم، ويمكنك فصل جزء من برنامج موجود، تعديله، إعادة ترجمته، واستبدال الملف الأصلي بنسختك المعدلة. (يوجد إضافة إلى المفككات التي تُخرج شيفرة بلغة assembly، مترجمات تحلل الملف وتولد شيفرة في لغة برمجة أعلى مثل لغة C).

مع أن الأمر يبدو مهمة تقنية صعبة، لكنها في الحقيقة ليست كذلك. حيث يعود مبدأ الهندسة العكسية إلى الأيام الأولى من الحوسبة الشخصية عندما قام المخرّبون باختراق مخططات حماية النسخ البرمجية للألعاب والتطبيقات. يوجد عدد من الأدوات للهندسة العكسية المتوفرة على الإنترنت، إضافة إلى البنية التحتية الكبيرة والتي تدعم أي شخص مهتم بالمشاركة في تفكيك برنامج تنفيذي ومن ثم إعادة جمعه مرة أخرى. وبالرغم من وجود عدد من الأشخاص اللامعين في مجال الهندسة العكسية، لكن ليس دائماً اللمعان مطلوب ليكون فعالاً.

(إذا كنت لا تزال غير مقتنع بأن نظام التشغيل Windows معرض لهذا النوع من المهاجمات، قم بزيارة الموقع www.rootkit.com للحصول على بعض المعلومات التقنية وأمثلة ذات شيفرة حقيقية. فقد تتفاجأ كثيراً).



قام أوروبي معروف باسم Fravia بإدارة موقع ويب لمدة خمس سنوات وقدم كمية كبيرة من المعلومات حول الهندسة العكسية. تضمن الموقع جولات تعليمية ومقالات من قبل عدد من "العاكسين" المحترفين حول تفكيك التطبيقات ومن ثم تعديلها. ومنذ عام 2000، حوّل Fjalar Ravia كل طاقته لاحتراف وسائل تحديد المعلومات على شبكة الإنترنت. ويمكن أن تزور موقعه www.fravia.com لكي تتجاوز عمليات البحث التقليدية عبر محرك Google. لا تزال نسخ الموقع الذي كان يتضمن مقالات حول الهندسة العكسية موجودة، ومن بينها الرابط /http://tsehp.cjb.net. (تذكر أن قرار حقوق النسخ الألفية الرقمية الأمريكي يرفض الهندسة العكسية).

إن طريقتك الدفاعية الرئيسة ضد هذا النوع من المهاجمات هي استخدام برنامج التجزئة MD5 لتوليد قيم التجزئة للبرامج التنفيذية والمكتبات التي قمت بتثبيتها حديثاً تماماً بعد أن قمت بتثبيت البرنامج من مصدر موثوق. وقم بالتحقق دورياً من هذه القيم مقارنة مع القيم الأصلية. فإذا كان هناك اختلاف في أحد القيم لسبب مجهول فقد يكون هناك ملف تم تعديله لأغراض التجسس.

من الهام أيضاً تشفير لائحة القيم أو تخزينها في مكان بعيد وآمن. فإذا أراد الجاسوس زرع ملف معدل في النظام، فقد يقوم أولاً بالبحث عن ملف يتضمن قيم التجزئة في القرص الصلب ومن ثم يغير قيمة التجزئة للملف بالإصدار المعدل. وعندما يتحقق المستخدم من قيم التجزئة. فلن يعرف أنه تم استبدال ملف أو أكثر بإصدارات معدلة.

أساليب: الواجب الوطني

بين حين وآخر، تظهر إشاعة عن شركة تقنية تتعاون مع الحكومة لتسهّل عليها التنصت على زبائنها، وهذا واجب وطني لمواجهة تحديات هذا العصر.

حيث تتمتع الوكالات الاستخباراتية بتاريخ طويل بخروجها عن القانون للتجسس على المواطنين الأمريكيين، وأحياناً مع التعاون الإرادي لمؤسسة أمريكية.

حيث أسست الوكالة السابقة لوكالة الأمن القومي NSA عام 1945 شراكة مع شركات RCA، ITT، و Western Union للحصول على نسخ من جميع رسائل التلغراف الداخلة والخارجة من الولايات المتحدة. لقبت هذه العملية بالاسم Operation Shamrock وكان يتم تسليم 150,000 رسالة شهرياً للوكالات الاستخباراتية لإجراء التحليل. استمر هذا التنصت غير القانوني حتى عام 1975، عندما تم كشف العملية أثناء مؤتمر الشهادة.

هل لا تزال أمور مماثلة تحصل؟ الجواب المؤكد عند الحكومة فقط، لكن توجد بعض الأخبار الحديثة المثيرة للاهتمام، سوف نعرض بعضاً منها.

في عام 1997، نشرت مقالة في جريدة سويدية أن تشفير البرنامج Notes لشركة Lotus كان معرضاً للتنصت من قبل الحكومة الأمريكية. وفي ذلك الوقت، كانت منتجات التشفير المشحونة إلى خارج الولايات المتحدة معرضة لعدد من القيود. بالرغم من أن التشفير ذو مفتاح 64 بت الذي عرضته شركة Lotus يمكن استخدامه في الولايات المتحدة، لكنه كان يمنع من التصدير إلى خارج الولايات المتحدة، ومن الواضح أن شركة Lotus عقدت صفقة مع الحكومة لتستطيع بيع المنتج ذو التشفير 64 بت لبلاد أخرى. وتم اقتباس أحد أقوال نائب رئيس الشركة Eileen Rudden قائلاً، "يكمن الاختلاف بين إصدار البرنامج الأمريكي والإصدار المصدّر الذي نقوم بتسليمه إلى خارج الولايات المتحدة في درجات التشفير. نقوم بتسليم مفاتيح بطول 64 بت لجميع الزبائن، لكن 24 بت من الإصدارات التي نقوم بتصديرها إلى الخارج محجوزة من قبل حكومة الولايات المتحدة. وهكذا تعمل حالياً." لم يكن السويديون يعلمون حول هذا الأمر ولم يكونوا سعداء. ولم يتم التعرف على الوكالة الحكومية التي حصلت على المفاتيح.

في شهر أيلول (سبتمبر) عام 1999، اكتشف باحث أمني أن واجهة برمجة التطبيقات التشفيرية لشركة Microsoft تضمنت مفتاحاً غير موثقاً يسمى "NSAKEY". وبدأت توجه

الاتهامات ضد الشركة بأنها وضعت أبواباً خلفية للحكومة في أنظمة التشغيل لديها لتسمح لوكالة NSA والوكالات الأخرى التحايل على الأمن. أنكرت شركة البرمجيات هذه المزاعم، وصرحت بأنه تم تسمية المفتاح بالاسم NSA لأن الوكالة NSA كانت هيئة المراجعة المسؤولة عن تصدير تقنية التشفير وكانت المفاتيح موجودة فقط من أجل الاستجابة لقوانين التصدير الأمريكية. كما صرحت الشركة أيضاً، "إن المفاتيح المسماة باسم NSA مجرد نسخة احتياطية لأحد المفاتيح التي نستخدمها لكي نستطيع تحديث مكونات التشفير، كما تمت إساءة اختيار الاسم، وهذه الاتهامات تدعو للسخرية لأن شركتنا ضد سياسة الحكومة في هذا المجال." (لكن ما يجدر قوله، أن وفقاً لتقرير الصحفي Wayne Madsen، خلال المنتدى التقني بين الوكالات الذي جرى عام 2001 في المعهد الوطني للمعايير والتقنيات، كشف مدير شركة Microsoft لأمن التشفير النقال بأنه قامت الشركة بمساندة مكتب ذو دوام كامل عند رؤساء وكالة الأمن القومي NSA وطاقم تقني بحت).

ومن الجدير بالملاحظة أنه في أثناء قضية الاحتيال الحاسبي والنشرة الأمنية في شهر حزيران (يونيو) عام 1995، كتب موظف سابق لوكالة الأمن القومي Madsen، بأنه قامت كلتا الشركتين Microsoft و Lotus بإنجاز اتفاقيات مع وكالة NSA تتعلق بميزات مرتبطة بالسرية في منتجاتها.

الفيروسات والديدان التي تجمع المعلومات

تتواجد فرص أكبر للتجسس حالياً مع الانتشار الواسع للإنترنت والتي لم تكن موجودة منذ خمس أو عشر سنوات. حيث تقدم الفيروسات والديدان احتمالاً واسعاً لكشف المعلومات بالغة الأهمية.

توجد عدة اختلافات بين هذه الأنواع من المهاجمات والحالات المنتشرة يومياً للفيروسات والديدان التي قد تواجهها وتقرأ عنها يومياً:

- تم تصميم شيفرة تجميع استخباراتية لجمع المعلومات سرياً. والهدف الوحيد من الشيفرة هو سرقة المعلومات والبقاء مخفياً، حيث يرغب المطوّر أن يتجنب منتجه الشعبية. وعلى خلاف كثير من الفيروسات والديدان، فإن الشيفرة متطورة وتم اختبارها جيداً. حيث يمكن أن تستخدم عدداً من الثغرات بدلاً من ثغرة واحدة للتأكد من نجاحها. وقد تحاول أيضاً تعطيل أي برنامج أمني قد يمنعها من إنهاء مهمتها.
- قد تستهدف الشيفرة أفراد أو منظمات محددة فقط. على خلاف الشيفرة التقليدية والانتهازية بطبيعتها، يمكن أن تكون شيفرة تجميع المعلومات انتقائية، مثل قذيفة ليزرية موجهة. قبل شن الهجوم، تقوم الشيفرة بالتحقق من عدد من الإدخالات في تسجيل النظام Windows لمعرفة إذا كان الحاسب يطابق التشكيل الجاني للحاسب الهدف. كما يتمتع

الهجوم المستهدف بفرص كشف أقل ، لأن الهجوم على عدد محدود من الحواسب والذي لا يتم كشفه لن يُسجل على رادار بائعي منتجات مكافحة الفيروسات التجارية. (كما يمكن أن يطبق هذا المفهوم للمهاجمات المستهدفة على مكونات غير تجسسية للصراع حول المعلومات، مثلاً وجود شيفرة تفحص تسجيل النظام للإصدار المحلي من النظام Windows المثبت وتهاجم فقط الحواسب التي تعمل على الإصدارات العربية).

مع أننا سوف نرى بعض الحسابات المؤكدة لشيفرة تجميع المعلومات المستخدمة من قبل منظمة حكومية ومتورطة في عملية التجسس ذات تكنولوجيا متطورة، لكن الاحتمال يتجاوز النظرية. حيث انتشر عدد من الأمثلة من الحياة الواقعية، مع تنوع درجات التعقيد، على شبكة الإنترنت في عدة حالات. ويمكن أن نفترض بأن مهاجمات التجسس المماثلة في طبيعتها، ومع أنها أصغرُ ومستهدفة أكثر، كانت قد وقعت.

الفيروسات (Viruses) والديدان (Worms)

الفيروس هو تطبيق ينفذ عملاً محدداً ويضاعف نفسه بإصابة البرامج أو الملفات الأخرى. الدودة مماثلة للفيروس لكنها لا تتضاعف عن طريق إصابة الملفات الأخرى. تكمن المشكلة في أنه يواجه بائعو برامج مكافحة الفيروسات وخبراء الأمن صعوبات في تحديد الفرق بوضوح بين هذين النوعين من الشيفرة الخبيثة. ودعونا بهدف المناقشة نعاملهما كليهما دون تمييز ولنفرض بأنهما تطبيقان يقومان بمضاعفة نفسيهما ويقومان بعمل ما دون علم مسبق من قبل المستخدم.

الهدف من الفيروس أو الدودة التي تجمع المعلومات هو نشر نفسها، جمع المعلومات من الحواسب المصابة، وإرسال رسالة راجعة إلى منشئها (يمكن أن يتم هذا عبر البريد الإلكتروني، بروتوكول FTP، خدمة المجموعة الإخبارية USENET، جهاز الفاكس، اتصال شبكي للطابعة، أو أية طريقة أخرى لإرسال البيانات إلكترونياً). يمكن استخدام التطبيقات بشكل واسع وبحيث يمكن أن تعمل ضد أي شخص تواجهه أو يتم استخدامها انتقائياً ضد أهداف محددة. فعلى سبيل المثال، إذا كنت تدير عملية تجسس ضد شركة IBM، فيمكنك استخدام فيروس يقوم بسرقة المستندات بعد التحقق أولاً من قيمة التسجيل لبرنامج Microsoft Office لتحديد الأعمال أو المنظمة التي تم تسجيل البرنامج باسمها. وإذا كانت قيمة المنظمة أحد اشتقاقات IBM سوف يقوم الفيروس بنسخ المستندات وإرسالها إلى مكان بعيد. أما إذا لم تتطابق القيمة مع الهدف، فقد يحذف الفيروس نفسه قبل أن يتضاعف ليتخلص من دليل وجوده (وربما لن يتضاعف بالأصل وينهي حلقة الاختبار في تلك النقطة).

عرفت شبكة الإنترنت فعلياً عدة فيروسات وديدان لتجميع المعلومات منتشرة خلال السنوات، ومن بينها التي سنناقشها في المقاطع التالية.

GALIGULA

في عام 1997، كتب Joel McNamara مقالة حول المهاجمات العملية التي يمكن شنها ضد برنامج PGP (www.privacy.com.au/pgpatk.html). وأحد الخيارات التي ذكرها McNamara باختصار هي فيروس تجسسي مصمم لجمع وسرقة المعلومات، وقد أثار احتمال الفيروس الذي ينتشر ويعمل على الحواسب التي تستخدم برنامج PGP. لكن الأمر الذي لم يكن يعلمه الكاتب أنه بعد عدة سنوات سوف يأخذ أحدهم المفهوم العام ويحوله إلى فيروس حقيقي.

وفي شهر شباط (فبراير) عام 1999، التقطت وسائل الإعلام قصة حول فيروس جديد ملقب بالاسم Galigula، مبرمج من قبل شركة Opic وهي حالياً توقفت عن العمل كمجموعة برمجة الفيروسات اسمها CodeBreaker. كان Galigula أحد فيروسات جمع المعلومات المعروفة، وكان يستهدف مستخدمي برنامج PGP. يقوم فيروس الماكرو المرتبط ببرنامج Word بالبحث عن وجود تطبيق PGP على القرص الصلب. فإذا تم إيجاد برنامج التشفير، سوف يؤسس الفيروس اتصال FTP إلى موقع بعيد و يقوم بإيداع نسخة من الحلقة المفتاحية الخاصة بالمستخدم. من المعقول أن يتم شن هجوم القاموس ضد الملف لتحديد إذا كان المستخدم يستخدم كلمة مرور ضعيفة. وفي حالة كانت كلمة المرور ضعيفة، بالتالي يمكن كشف رسالة إلكترونية مرسلة من قبل ذلك المستخدم.

وقد صرحت شركة Opic في مقابلات صحفية بأن الهدف من الفيروس هو فقط مجرد برهان للمفهوم، مصمم لإظهار أنه يمكن كشف برنامج PGP. ليس معروفاً كمية الحلقات المفتاحية لبرنامج PGP التي تم نسخها أو إذا تم شن أية مهاجمات ناجحة ضدها. (يمكنك استعراض إصدار مؤرشف للصفحة الرئيسة لشركة Opic غير الموجودة حالياً لكي تحصل على المعلومات الأصلية حول الفيروس، على الرابط:

.(http://web.archive.org/web/19990221015817/http://members.tripod..com/opiccb/index.htm

MARKER

بعد مرور عدة أشهر من نشر فيروس Galigula، ظهر فيروس آخر مبرمج من قبل مجموعة CodeBreakers. هــذا الفيــروس يسمى Marker (بسبب النص في بداية الشيفــرة وهو "this is a marker") وقام باسترجاع اسم مالك نسخة برنامج Microsoft Word ويقوم

بتسجيله عندما يصيب الفيروس الهدف. وفي بداية كل شهر، سوف يحاول الاتصال بموقع FTP للمجموعة CodeBreakers وإيداع المعلومات التي جمعها. مرة أخرى، يبدو أن هذا الفيروس مصمم كبرهان للمفهوم لتعقب انتشار ونسبة الإصابة. وقد توقف مؤلف هذا الفيروس، والذي يسمى Spooky والبالغ من العمر سبعة عشر عاماً، عن العمل عمداً بعد أن علم بأن هذا الفيروس أصاب منظمات مثل Blue Cross. وقد صرح أحد المرات على موقعه "يجب أن يكون لكل شيء حدود، وأعتقد أني وجدت حدي."

SIRCAM

انتشرت دودة SirCam، في شهر تموز (يوليو) عام 2001، بشكل هائج على شبكة الإنترنت. حيث فتح كثير من الأشخاص دون قصد ملفاً مرفقاً مرتبطاً برسالة إلكترونية محتواها، " Hi! How are you? I send you this file in order to have your advice. See you later. Thanks." (بالتأكيد قامت الدودة بسحب عناوين البريد الإلكتروني من دفتر العناوين في النظام Windows بحيث بدت الرسالة وكأنها من أحد ما تعرفه، لكن بصراحة، من يقوم بكتابة رسائل صيغتها كتلك من بين أصدقاءك، معارفك الشخصية، أو زملائك في العمل؟ هذا مثال ممتاز لتنفيذ الهندسة الاجتماعية).

عندما يتم فتح الملف، سوف تنسخ الدودة مستنداً تختاره عشوائياً (ذو التنسيق DOC، XLS، أو ZIP.) من الحاسب المصاب، وترفق هذا المستند إلى رسالة إلكترونية ومن ثم تحاول أن تضاعف نفسها وذلك بإرسال الدودة مع الملف المرفق إلى جميع الأشخاص في دفتر العناوين.

قامت الدودة SirCam لعدة أشهر بعرقلة شبكة الإنترنت، مرسلة رسائل إلكترونية مصابة تتضمن مستندات أعمال أو مستندات شخصية إلى الغرباء. وقد كان المركز الوطني لحماية البنية التحتية التابع لمكتب التحقيقات الفدرالي أحد ضحايا هذه الدودة. وقد أكد مكتب التحقيقات أنه لم يتم نشر أية مستندات سرية أو هامة.

أساليب: فيروس Dalai Lama

في أيلول (سبتمبر) عام 2002، اتهم مدير مركز الأبحاث الحاسبية التيبيتي في Dharmsala، الهند الحكومة الصينية بتصميم ونشر فيروس مبرمج من أجل سرقة المعلومات. وقد تم إرسال الفيروس إلى ثلاث جماعات أخرى من الناشطين حول العالم، والتي ظهر بأنها نشأت في مركز الأبحاث. وفقاً لتصريحات المدير، تم تصميم الفيروس ليرسل البيانات إلى ستة عناوين إلكترونية في الصين، ومن بينها الجامعات والمؤسسات الحكومية. فرضياً، أرسل مرتكبو الجريمة الرسالة الإلكترونية التي تضمنت الفيروس في مرتين مختلفتين.

أنكرت الحكومة الصينية تورطها، مصرحة بأن الحكومة تعارض دوماً نشاطات القراصنة الإلكترونيين. ولم تظهر نسخ من الفيروس على الإنترنت لكي يتم التأكد بشكل منفصل فيما إذا كان الفيروس يهدف للتجسس أم لا. يبدو من الوصف أنه قد يكون هذا الفيروس من النوع العام للفيروس SirCam، والذي لم يكن موجهاً بشكل خاص إلى المنظمات التي تدعم Dalai Lama. لكن مع معرفة مقدار الكراهية التي يملكها الصينيون ضد الحركة التبتية الحرة واهتمام الحكومة بتقنيات الصراع حول المعلومات، لذلك فإن الهجوم المستهدف هو أحد الاحتمالات الممكنة.

BADTRANS.B

في شهر تشرين الثاني (نوفمبر) عام 2001، خدعت دودة أخرى لجمع المعلومات مستخدمي الإنترنت. تم تسمية الدودة بالاسم Badtrans.B (شكل آخر للدودة Badtrans التي ظهرت قبلها في شهر نيسان (أبريل)، وتعرض الأشخاص الذين فتحوا الملف المرفق المصاب لتجسس يتحمل ضغطاً شديداً. حيث بعد تنفيذ الدودة تقوم بمضاعفة نفسها بإرسال نسخ منها إلى عناوين البريد الإلكتروني المخزنة في دفتر العناوين لبرنامج Outlook Express. كما كانت تثبت مسجل مفاتيح مصمم لسرقة كلمات المرور الخاصة بالبريد الإلكتروني، بروتوكول FTP، خدمة Telnet، وحساب الويب. إضافة إلى كلمات المرور تم تسجيل أي شيء يقوم المستخدم بطباعته.

بعد أن جمعت الدودة Badtrans.B البيانات المختلسة، تقوم بإرسالها إلى عنوان واحد بين 17 إلى 22 عنواناً إلكترونياً مختلفاً، وكلها حسابات مجانية للبريد الإلكتروني، حيث أحد العناوين الوهمية التي تم إرسال البيانات إليها هي *#!_my_p$#**%@ijustgotfired.com. حيث بدأ الحساب باستقبال الرسائل الإلكترونية من الحواسب المصابة منذ ظهيرة الرابع والعشرين من تشرين الثاني (نوفمبر). وقد وصل حجم الرسائل إلى أكثر من حجم الصندوق الوارد، وتم تعطيل الحساب. وفي اليوم التالي عندما تحقق مدير النظام من السجلات محاولاً أن يعرف سبب البطئ الكبير للملقم، اكتشف أن الحساب استقبل أكثر من مائة رسالة إلكترونية كل دقيقة. وقد كشفت فحوصات لاحقة بأن الدودة Badtrans.B أرسلت معلومات سرية إلى الحساب من أكثر من 100000 حاسب مصاب خلال اليوم الأول فقط.

اكتشف مزود خدمة الإنترنت MonkeyBrains.net والذي كان يستضيف المجال ijustgotfired.com ماذا كان يحصل وبدأ يجمع الرسائل الإلكترونية. وقد صمم Rudy Rucker الأصغر مالك الشركة قاعدة معطيات ذات صفحة ويب في المقدمة، حيث يمكنك أن تستعرض البيانات المكشوفة. لكن سرعان ما انتشرت أخبار الموقع، وقام Rucker بتعطيل بعض خيارات "الكشف الكامل" للبيانات.

وقد علم مكتب التحقيقات الفدرالي أيضاً عن Rucker وطالبه بنسخة من عدة جيغا بايتات من البيانات المكشوفة التي استقبلها المزود MonkeyBrains، ومن ضمنها أكثر من مليون ونصف من أزواج كلمات المرور/الحسابات، تقريباً ستة ملايين من جلسات تسجيل المفاتيح، وأكثر من 300,000 عنوان بريد إلكتروني للأشخاص الذين تمت إصابتهم بالدودة. وقد تجاهل Rucker سرية مئات الآلاف من الأشخاص الذين تم خداعهم مسبقاً، وقام بكشف بياناتهم مرة أخرى دون أن يملك رخصة.

دودة Badtrans.B هي مثال تقليدي للسرعة التي ينتشر بها فيروس أو دودة مرفقين برسالة إلكترونية وقوتها عندما يتم تصميمها خصيصاً لجمع المعلومات. لا تزال تتوفر نسخة ناقصة من قاعدة معطيات Rucker على الرابط /http://badtrans.monkeybrains.net فهي مثيرة للاهتمام.

المستقبل

من البديهي أنه كلما تم اكتشاف نقاط ضعف جديدة لنظام التشغيل Windows، سوف يستفيد مبرمجو الفيروسات والديدان منها. علاوة على ذلك توجد تقنيتان ناميتان والتي يمكن أن تتيحا فرصاً أكبر لمهاجمات شيفرة تجميع المعلومات.

- **الأجهزة النقالة:** حتى الآن، لم يستهدف مبرمجو الفيروسات الأجهزة النقالة مثل الهواتف الخلوية، لكنها مجرد مسألة وقت قبل أن يحصل هذا. لكن بما أنه تم تضمين وظائفية المساعد الرقمي الشخصي PDA ضمن عدد متزايد من الهواتف الخلوية، يمكن أن تتحقق احتمالات وجود فيروس تجسسي يستطيع سرقة أدلة الهاتف، التقويم، ومعلومات أخرى.
- **"عنوان IP في كل مكان":** مع أن طموحات امتلاك جميع أنواع المنتجات لتمكين عنوان IP للعمل معاً ضمن شبكة في المترل أو العمل، هي مجرد نظرات إلى الأفق، لكنها تقدم احتمال تجسسي كبير جداً. حيث إضافة إلى إمكانية كشف المعلومات من جميع الأجهزة يمكن أن يعرّض وجود ثغرة وحيدة في أحد الأجهزة كامل الشبكة للخطر. ومع الأخذ بعين الاعتبار أن الإجراءات الأمنية في التقنيات الجديدة تحوي دوماً بعض نقاط الضعف، لكن عندما تتوفر أجهزة "عنوان IP في كل مكان" عليك أن تأخذ احتياطاتك.

الإجراءات المضادة

بالرغم من أن برامج مكافحة الفيروسات وتطبيقات حصان طروادة وتطبيقات جدار الحماية هي خط الدفاع الأول ضد الفيروسات والديدان التي تجمع المعلومات، لكن الخصم المتطور بالتأكيد سوف يصنع شيفرة ما لتجاوز الكشف من قبل المنتجات الأمنية التجارية.

يمكنك تقليل فرص وقوعك ضحية هذه الأنواع من المهاجمات عن طريق امتلاك سياسة أمنية قوية (وخاصة عندما يتعلق الأمر بالتعامل مع البريد الإلكتروني) واستخدام برامج خدمية تتعقب اتصالات الشبكة، إدخالات التسجيل Registry، وكتابات الملفات. (تمت مناقشة هذه البرامج والسياسات في فقرات " الإجراءات المضادة " للفصلين الثامن والتاسع).

توجد طريقة أخرى لتقليص أخطار هذه المهاجمات وهي عدم تخزين المعلومات بالغة الدقة على حواسب ذات اتصالات شبكية والتي يمكن أن تقدم قناة لهجوم عدواني. ولتحقيق هذا، استخدم الجيش ووكالات الاستخبارات مفهوماً يسمى "أحمر/أسود، Red/Black" حيث تعتبر الحواسب والشبكات الحمراء آمنة (فقد تتضمن واقي TEMPEST، شبكات خاصة ظاهرية مشفرة، وإجراءات دفاعية أخرى). أما الشبكات والحواسب السوداء فيمكن أن تكون غير آمنة، لذلك يمكن أن تتعرض المعلومات التي تتضمنها للخطر. ويتم فصل الأنظمة الحمراء عن الأنظمة السوداء لتجنب تسرب المعلومات السرية من الأنظمة الحمراء إلى الأنظمة السوداء غير الآمنة.

لا تحتاج لتكون موظفاً عند رؤساء وكالة NSA لكي تطبق هذا الإجراء، حيث يتألف النظام "أحمر/أسود" البسيط من حاسب أسود وحيد متصل بالشبكة مثل شبكة الإنترنت وحاسب أحمر غير متصل بأي شبكة. ويمكن نقل أية رسائل مشفرة مستقبلة من قبل الحاسب الأسود غير الآمن يدوياً إلى الحاسب الأحمر الآمن وذلك باستخدام أقراص، بطاقة ومضية، أو قرص صلب USB.

يتم استخدام الحاسب الأحمر من أجل تشفير وفك تشفير الرسائل الإلكترونية والتعامل مع البيانات الهامة (يمكن تمرير ملفات البيانات فقط من الحاسب الأسود إلى الحاسب الأحمر، ويفضل أن يكون تنسيقها لا يدعم فيروسات الماكرو). يقلص استخدام هذا الحاسب أية تهديدات شبكية محتملة لكشف المعلومات على الحاسب الآمن. كما يجب أن يحوي كلا الحاسبين برمجيات مكافحة الفيروسات وتطبيقات حصان طروادة، تطبيق جدار ناري، وبرمجيات أمنية أخرى. (ومع أن هذه الطريقة ليست مناسبة للاستخدام مثل استخدام حاسب واحد، لكنها تستطيع التغلب على معظم المهاجمات البعيدة في بيئة مليئة بالأخطار).

كاميرات المراقبة

إذا كنت تملك وصولاً فيزيائياً للهدف، فإن من إحدى طرق كشف المعلومات (ومن بينها كلمات المرور) هي استخدام كاميرا المراقبة. حيث استخدم مكتب التحقيقات الفدرالي كاميرات فيديو مخفية في عدد من التحقيقات التجسسية لمراقبة نشاطات الجاسوس المشتبه به. قم

باختيار موقع مخفي (في السقف مثلاً)، وجّه الكاميرا إلى شاشة الحاسب ولوحة المفاتيح، وانتظر حتى تسجل الكاميرا أفعال الهدف.

ربما قد تستخدم بعض أنواع الأجهزة التي تدمج "كاميرا على رقاقة"، لذلك دعونا نناقش باختصار هذه التقنية. تستخدم كاميرات الفيديو والكاميرات الرقمية حساسات تقوم بتحويل الضوء إلى شحنات كهربائية. يوجد نوعان من الحساسات: جهاز مرتبط بالشحنات CCD (charge couple device) وأكسيد معدن نصف ناقل متتام CMOS (complementary metal oxide semiconductor).

- حساس CCD هو مجموعة من الديودات الصغيرة جداً والتي تحول الفوتونات (الضوء) إلى إلكترونات (الشحنات الكهربائية). يمكن أن يكون هناك عدة مئات الآلاف من الديودات على رقاقة واحدة.
- تعمل حساسات CMOS بشكل عام بنفس طريقة حساسات CCD، لكنها حالياً أقل تحسساً بعشر مرات ولا تستطيع التقاط الصور بدقة عالية. ميزاتها الأساسية هي تكلفة تصنيعها أقل وتستهلك طاقة أقل بكثير.

كما تتميز تجهيزات مراقبة الفيديو السلكية المخفية (تسمى أحياناً CCTV اختصاراً للعبارة Closed Circuit Television) بأنها لا تخضع إلى إشارات تردد الراديو التي تكشفها، على خلاف أجهزة التنصت الصوتية التي تقوم بنقل إشارات تردد الراديو ويمكن أن يتم كشفها بسهولة (حسب نوع الجهاز) باستخدام محلل الطيف أو ترس مخصص لكشف أجهزة المراقبة. أحد طرق كشف الكاميرات المخفية، دون قلب الغرفة رأساً على عقب، هي استخدام مصوّر حراري محمول ونقال. حيث يسجل كل من الكاميرا ومصدر الطاقة التوقيع الحراري المرئي على شاشة عرض المصوّر، حتى لو كانت الكاميرا مخفية أو موضوعة ضمن شيء ما. (لا يمكن تخمين النتيجة إذا كنتَ مستهدفاً من قبل وكالة حكومية أو استخباراتية، والتي قد تستخدم تجهيزات مخصصة للمراقبة والتي تستطيع التغلب على وسائل الكشف القياسية).

إجراءات مضادة: TSCM (Technical Surveillance Countermeasures)

الإجراءات المضادة للمراقبة التقنية (TSCM) وهي علم وفن كشف والتغلب على أجهزة المراقبة. تقليدياً، كان هذا المصطلح يشير إلى التنصت الصوتي، لكن يمكن تطبيقه الآن على

أي نوع من تقنيات المراقبة، ومن ضمنها الفيديو. (يمكن استخدام المراقبة الصوتية أيضاً ضد الحواسب. حيث كشف البريطانيون خلال عملية ENGULF في الخمسينيات و الستينيات الاتصالات الفرنسية والمصرية عن طريق كشف الضجيج بوساطة تعيين آلات التشفير المستخدمة لتشفير الرسائل. يمكن شن مهاجمات من هذا النوع ضد الطابعات النقطية ولوحات المفاتيح).

هناك مورد ويب ممتاز للتعلم حول أدوات وتقنيات الإجراءات المضادة للمراقبة هو موقع Granite Island Group TSCM على الرابط www.tscm.com. حيث تتم استضافة الموقع من قبل James Atkinson، وهو محترف TSCM جدير بالاحترام، كما يتضمن الموقع كمية مذهلة من المعلومات المفصلة حول التنصت ومكافحة التنصت.

كاميرات الويب

مع أن كاميرات الويب (وهي كاميرات صغيرة مصممة لبث فيديو حي عبر الإنترنت) ليست تقنية تجسسية متطورة، لكن بالتأكيد يمكن استخدامها للمراقبة أو مكافحة المراقبة. حيث تعلمت في الفصل التاسع حول تطبيقات حصان طروادة والتي تستطيع أن تتنصت على خرج كاميرا الويب وإرسال ملفات الفيديو إلى الجاسوس. كذلك في الفصل الحادي عشر، رأيت أنه بإمكان جاسوس يملك تجهيزات مناسبة التنصت على كاميرات الفيديو اللاسلكية. فإذا كنت تستخدم كاميرا ويب أو نوعاً مماثلاً من الكاميرات، تذكر دوماً أنه يمكن أن يتم استخدامها ضدك.

كما تستطيع أيضاً، إضافة لمراقبة إشارة الفيديو عن بعد من خلال كاميرا مستخدم ساذج، أن تتولى مهمة المراقبة المحلية. يتوفر عدد من التطبيقات البرمجية والتي يمكن أن تحول كاميرا الويب إلى نظام مراقبة يقوم بمراقبة منزلك أو مكتبك. تستخدم هذه التطبيقات خوارزميات تحسس الحركة لالتقاط الصور حالما يتحرك شيء ما أو أحد ما ضمن مجال رؤية الكاميرا (يمكن توجيه الكاميرا إلى داخل الغرفة أو إلى الخارج عبر النافذة). عندما تتحسس الكاميرا للحركة، يمكن أن ينبهك البرنامج اختيارياً عبر البريد الإلكتروني، وحتى يمكنك استعراض الصور في الزمن الحقيقي من مكان بعيد عبر شبكة الإنترنت باستخدام بعض التطبيقات.

تتضمن بعض المنتجات البرمجية الشائعة لكاميرات الويب ما يلي:

- **Digi-watcher**: تتضمن هذه الحزمة البرمجية وظائف تسجيل شاملة، وتتوفر على الرابط www.digi-watcher.com بسعر 39 دولاراً أمريكياً.
- **InetShepard**: ويسجل الصوت والصورة معاً ويمكن التحكم به عبر الهاتف، يمكنك تحميله من الرابط http://inetshepard.com، تبلغ تكلفته لكاميرا واحدة 35 دولاراً أمريكياً.



لمزيد من المعلومات حول عدد من المنتجات التجارية الأخرى لكاميرات الويب، اتبع الرابط www.webattack.com/shareware/webpublish/swwebcam.shtml.

بالرغم من أن نوعية الصورة لكاميرا الويب لا تتطابق مع دقة تلفاز البث، لكنها قد تكون كافية لأنواع مختلفة من نشاطات التجسس. لكن إذا كنت تحتاج إلى كاميرا خفية أو كاميرا قادرة على إخراج صور ذات دقة عالية، يمكنك شراء كاميرا مصممة خصيصاً للمراقبة.

أدوات التجارة: كاميرات المراقبة العامة

تظهر كاميرات مراقبة الفيديو بأعداد متزايدة على أعمدة الشوارع وعلى الأبنية في جميع أنحاء الولايات المتحدة. غالباً يتم استخدام خرج الفيديو من قبل قوى القانون للاستجابة للجرائم قبل أن يبلّغ عنها المواطنون، الاستفادة منها كدليل، وبناء علامات مساعدة في القضايا الجنائية.

يمكن أن تكون كاميرات المراقبة غير مراقَبة (مثل آلة الصرافة المؤتمتة في المصرف حيث يتم تخزين الفيديو على شريط) أو تتم مراقبتها بشكل نشط من قبل شخص. يمكن تحريك الكاميرات المراقبة باستخدام جهاز تحكم عن بعد، بحيث يستطيع موظف الأمن تغيير زاوية الكاميرا أو يعدل العدسة للتركيز على فرد أو نشاط ما.

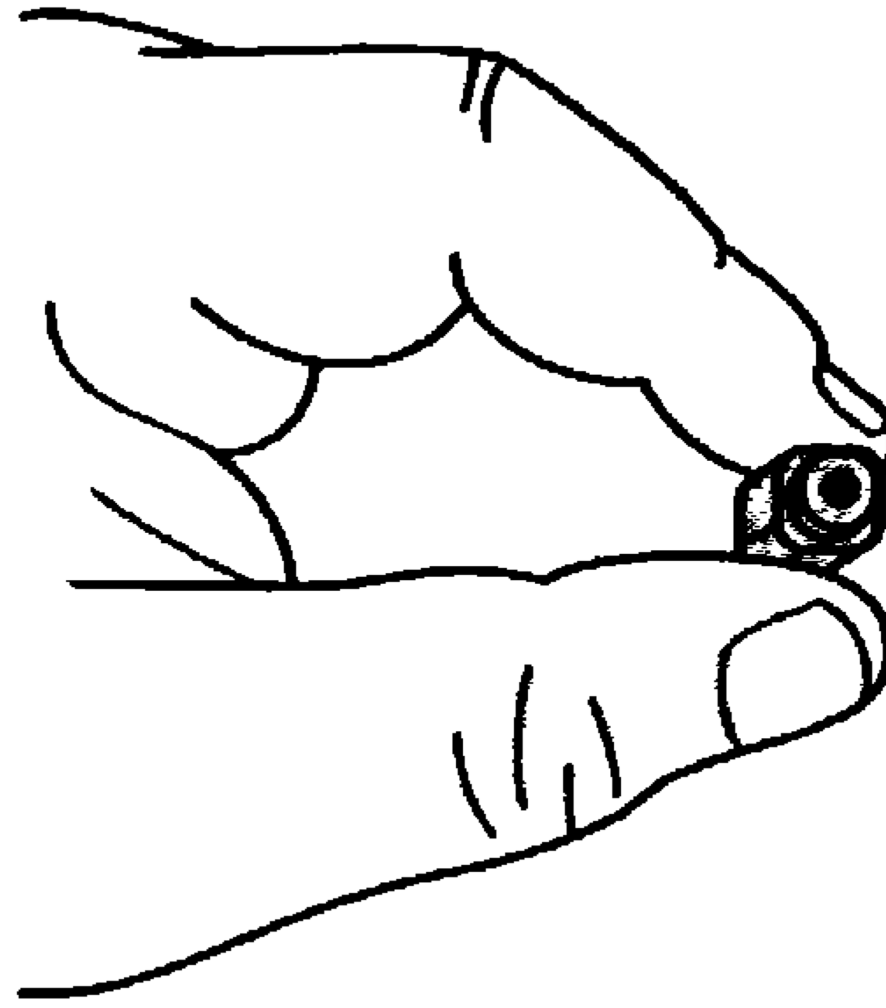
أصبحت كاميرات المراقبة جزءاً أساسياً من البنية الاجتماعية في بريطانيا (وهي البلد الأول في مراقبة الفيديو العامة)، تقدر المجموعات اللا ربحية أنه توجد حوالي 1.5 مليون إلى 2 مليون كاميرات تلفاز مغلقة الدارة في بريطانيا. وتقدر مجموعة الحراسة Privacy International والتي مقرها في لندن بأن الحكومة أنفقت أكثر من 9 مليارات دولار أمريكي على المراقبة خلال 15 سنة الماضية.

لنعطيك فكرة حول شيوع أجهزة المراقبة هذه في الولايات المتحدة، قام مشروع كاميرا المراقبة لمدينة نيويورك بتعريف وتسجيل مواقع كاميرات المراقبة في الأماكن العامة حول نيويورك. حتى الآن تم التعرف على أكثر من 2,300 كاميرا مراقبة في شوارع نيويورك والتي تلتقط المشاة العابرين المجهولين وراكبي الدراجات النارية. (يتضمن هذا الرقم الكاميرات الخارجية فقط، ولا تدخل الكاميرات داخل المباني ضمن العدد). يمكنك الحصول على خرائط ومزيد من المعلومات حول كاميرات المراقبة المعروفة في مدينة نيويورك من موقع الويب الخاص بهذا المشروع، على الرابط /www.mediaeater.com/cameras.

مع أن مؤيدي المراقبة يصرحون بأن الكاميرات تساعد على تقليص واكتشاف الجريمة، إلا أن مؤيدو الخصوصية غير متأكدين من هذا الأمر ويعتبرون الكاميرات خطوة أخرى لتعرية الخصوصية الفردية. لكي تحصل على مزيد من المعلومات عن الآثار الخصوصية لكاميرات المراقبة في الأماكن العامة، اتبع الرابط /www.epic.org/privacy/surveillance.

كاميرات المراقبة التجارية

مع أنه يمكن استخدام كاميرات الويب لأهداف التنصت، لكن من الأفضل غالباً استخدام كاميرا تم تصنيعها بشكل أساسي لأهداف المراقبة. تكون هذه المنتجات التجارية أصغر من كاميرا الويب (انظر الشكل 2-13)، وتتمتع بدقة أفضل، ويمكن أن تملك ميزات متقدمة مثل التقاط الصور في الظلام. يمكن إخفاء كاميرات المراقبة الصغيرة في أي مكان يمكن أن يخطر في تفكيرك مثل الساعات، الترموستات، أجهزة الراديو، السماعات، الخ.



الشكل (13-2) كاميرا فيديو مصغرة أبيض وأسود من نوع SuperCircuits. أبعادها 9.5 × 16 مم، افتراضياً يمكن إخفاء الكاميرا في أي مكان وتنتج إشارة فيديو NTSC نظامية. سعرها 99 دولاراً أمريكياً، ويمكن أن يشتريها الجواسيس ذوي الميزانية القليلة.

يتم تصميم معظم هذه الكاميرات لتستخدم مصدر خارجي لطاقة البطارية وتخرج إشارة فيديو إلى جهاز تسجيل من نوع VCR. كما تتوفر كاميرات صغيرة لاسلكية تقلص الحاجة إلى ربط الكاميرات مباشرة إلى المسجل.



تعتبر شركة SuperCircuits مصدراً معروفاً لمراقبة الفيديو لوكالات قوى القانون والصناعات الأمنية. يزود البائع الكاميرات، المسجلات، وأي شيء قد تحتاج إليه لإدارة مراقبة الفيديو. يتوفر دليل على شبكة الإنترنت من الرابط www.supercircuits.com.

توجد حالياً، بالإضافة إلى عدة قوانين فدرالية منعت بيع واستخدام أجهزة التنصت الصوتية، عدة قيود على المصّنعين ومبيع تجهيزات مراقبة الفيديو. تتوفر الكاميرات المتطورة وأجهزة تسجيل الفيديو بسهولة لأي شخص ضمن أسعار معقولة. (تذكر احتمال وجود قوانين سرية ضمن الولايات والتي تحظر تسجيل بعض النشاطات المحددة).

تلخيص

فيما عدا وقوع كارثة ما قد تدمر جميع الأجهزة الإلكترونية، سوف يكون هناك دوماً تجسس حاسبي يحيط بنا. وبما أن اعتمادنا في حياتنا اليومية على الحواسب أخذ يتصاعد، سوف يزداد احتمال الإساءة التي قد نتعرض لها من قبل الجواسيس والمتطفلين.

لا يعني هذا الكلام أنه يجب أن تلبس رقاقة معدنية على رأسك، أن تستخدم مشوش أصوات لاتصالاتك الهاتفية، وأن تبدأ بشراء تجهيزات TEMPEST الفائضة من خلال خدمة eBay. حيث في أغلب الأوقات لا تحتاج إلى أن تقلق حول بعض هذه التقنيات التجسسية المتقدمة، بالطبع ما لم تكن هدفاً لوكالة قوى قانون فدرالية، وكالة حكومية استخباراتية، أو منظمة أخرى ممولة جيداً.

بالرغم من أن الكينونات الممولة جيداً (حيث يتم تقدير ميزانية وكالة الأمن القومي NSA بأكثر من 13 مليار دولار أمريكي سنوياً) تملك موارد تتقدم تقريباً بفترة 15 إلى 20 سنة عن العالم المدني في بعض أنواع التقنيات الأمنية وتملك جميع أنواع الألعاب المثيرة التي لا نعلم بوجودها، لكن الاقتصاد يقول أنه لا يمكن استخدام هذه الممتلكات بفعالية ضد عدد كبير من الناس بشكل يومي. (خذ برنامج ECHELON كمثال: في نهاية جميع الاتصالات التي تم اعتراضها، لا يزال البرنامج يحتاج إلى محلل بشري لفحص هذه الاتصالات ومعرفة فيما إذا كانت جزءاً من لغز كبير).

كما أن المنظمات الممولة جيداً والمؤجرة لجمع المعلومات والمراقبة ليست تلك الآلات الجبارة التي لا تخطئ والتي ترغب الصناعات ووسائل الإعلام اعتبارها كذلك. فكر قليلاً بعدم قدرة الحكومة على اكتشاف ومنع هجمات الحادي عشر من أيلول (سبتمبر) المثيرة للجدل، وحقيقة عدم وقوع أية اعتقالات في الرسائل المتبادلة التي تبعت هذا الحدث، أو النجاحات المحدودة نسبياً في حربها ضد الإرهاب على الرغم من إنفاق مبالغ طائلة على هذه القضية.

عندما تفكر بإمكانية تطبيق التجسس الحاسبي المتقدم ضدك، دائماً اتبّع التعقل في اتخاذ الإجراءات الأمنية (وتذكر الاختلافات بين المهاجمات الممكنة والمحتملة)، لكن لا تقم أبداً بتقليل قيمة خصمك.

جدول المحتويات

2

3

أعمال الحقيبة السوداء 71

4

اختراق النظام 97

5

6

7

8

9

10

11

13

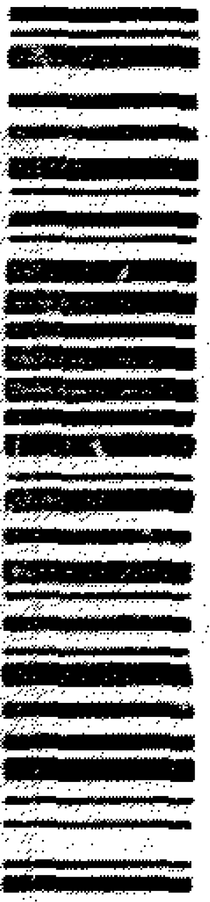
WATCH OUT FOR SPIES

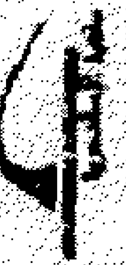
أنت لا تحتاج إلى تصريح سري للغاية أو خلفية قوية في التشفير أو أمن المعلومات لكي تستطيع أن تقرأ الكتاب.

إذ سوف يجد القرّاء التقنيون وغير التقنيين معلومات مفيدة تساعدهم على تفهم مخاطر التجسس بشكل أفضل وكيفية حماية حواسبهم من جميع الأنواع المختلفة من هجمات الجواسيس.

من المواضيع التي يغطيها الكتاب:

- تحصين حاسبك من الوقوع ضحية التجسس
- التعرف على نقاط الضعف في مستعرضات الويب والبريد الإلكتروني ودفاتر العناوين وسبل تقويتها
- معرفة قدرات الجواسيس في استغلال جهاز فاكس عادي أو هاتف جوال أو البريد الصوتي والكاميرا الرقمية
- أعمال الحقيبة السوداء المشوقة التي يقوم بها رجال الاستخبارات وطرق اختراق الأمن الفيزيائي لأي نظام.
- الاستخدام الصحيح لكلمات المرور ونقاط الضعف المرتبطة بسوء استخدامها، وكيفية اختراق كلمة مرور في نظام حاسبي.
- استخدام التشفير لحماية جميع أنواع المعلومات الحساسة لديك.
- التعرف على برامج مسجلات المفاتيح من أجل ... النشاطات المطبقة على لوحة المفاتيح بشك...
- استخدام تطبيقات حصان طروادة للتطفل على ... وكيفية حماية نفسك منها.
- التنصت على الشبكات السلكية واللاسلكية ... الأجهزة الالكترونية والإجراءات المضادة المرتبطة به...
- أنواع الجواسيس والقوانين المرتبطة بجريمة التجس...
- التمييز بين التنصت الالكتروني الشرعي وغير الش...









http://www.raypub.com